UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

GATEGUARD, INC.

Plaintiff,

v.

AMAZON.COM, INC.,
AMAZON.COM SERVICES, INC.,
AMAZON.COM SERVICES, LLC,
AMAZON LOGISTICS, INC.
RING, LLC

Defendants.

Civil Action No. 21-cv-9321 (JGK)

SECOND AMENDED AND CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff GateGuard, Inc. ("GateGuard" or the "Company") by and through its attorneys, Quainton Law, PLLC, for itself and on behalf of all others similarly situated, as and for its Complaint against Defendants Amazon.com, Inc., Amazon.com Services, Inc., Amazon.com Services, LLC, Amazon Logistics, Inc. (collectively, "Amazon") and Ring, LLC (collectively, with Amazon, the "Defendants"), alleges and states as follows:

INTRODUCTION

1. This is an individual and class action for damages, documented with photographic and video evidence, resulting from Amazon's illegal pattern of tampering with intercom and access control devices in multifamily residential buildings in New York and across the nation, while lying to or deceiving low-level building personnel to gain access to buildings without the owners' knowledge or consent and install its supposedly "free" door opening device – the Amazon "Key for Business -- that comes with the hidden costs of damage to other parties' property.

3. To gain access illegally to residential buildings, Amazon either directly or through intermediaries forges names onto contractual documents, lies orally to low-level employees, allows superintendents at individual properties to "authorize" the installation of the Key for Business on a portfolio-wide basis, enters phony contact information, such as make-believe email addresses, pretends to have authorization it does not have, and even dispenses with any written documentation of any kind in its hast to get its product installed in the classic "break doors first - explain afterwards" strategy of parties seeking to grow market share without regard to legal niceties.

2. As a result of these practices, GateGuard and individual property owners frequently have no idea that the Key for Business is installed at GateGuard buildings, and when the intercom ceases functioning because of a Key for Business-related problem – such as a short-circuit of the intercom because of the installation of the Key for Business or the excess power load created by the installation of the Key for Business – GateGuard suffers the loss of customers and access to customers' portfolios of properties, lost opportunities to generate maintenance revenue and market add-on services, lost intangible benefits such as free advertising, and the loss of goodwill and reputational damage, and property owners suffer damage to their amplifiers, magnetic door strikes and other property

3. In addition, Amazon has also posed as a GateGuard client through one of its so-called "channel partners" – the entities that operate at Amazon's direction to strong arm potential clients into accepting the installation of a competing device, the Amazon Key for

Business, or "Amazon Key" – so as to study the features of the GateGuard device at its top secret research laboratory and has also interfered with GateGuard's contractual relations and prospective economic advantage, committed computer fraud, misappropriated trade secrets, converted property to its own use, and unjustly enriched itself. GateGuard is also seeking an injunction permanently enjoining Amazon from taking any further action to tamper with any intercom devices installed in multifamily residential buildings in New York without the consent of the device owner and the building owner/manager or to engage in any further pattern of surreptitious installation of its key device without the property owner's knowledge and consent.

4. Founded in 2016, GateGuard is a startup company that develops, manufactures and sells security technology for multi-tenant apartment buildings.

5. One of GateGuard's primary offerings is its "AI Doorman" intercom device, which was first released in 2016.

6. GateGuard's intercoms offer unique features and capabilities that enable building managers to autonomously track everyone who enters, buzzes, or uses a guest code. These features alert building managers to forbidden activities such as illegal subletting, use of residential apartments as dormitories, unauthorized or non-compliant group activities and other threats to the safety and property of residents and landlords alike.

7. GateGuard's intercoms also generate real-time logs of these activities managers can view, filter, and print from any mobile phone, tablet, or computer, which are accessible via built-in cellular modems that connect the units to the Internet. GateGuard thus constitutes a valuable repository of client data of great interest to a business such as Amazon.

8. Moreover, because Amazon obtained access to a physical device designed to be marketed to a property manager (which Amazon falsely pretended to be through its channel partner acting at its direction), Amazon software engineers could get access to the design, components,

processing, communications, messaging, performance – in physical, functional, and logical realms – of the GateGuard system by studying the GateGuard device at an ultra-secret research and development lab, on the flimsy pretext that it was appropriating the GateGuard device, in violation of the GateGuard contract its channel partner accepted, for "trouble-shooting purposes." Obviously, had Amazon truly been interested in "trouble shooting" they would have been honest and cooperative with GateGuard, which they were not.

9. The GateGuard system as a whole includes an intercom, mobile app, web-based online platform, servers, communications devices, and operational data, all of which were uniquely designed to provide an access control solution used by tenants/visitors, property owners/managers, and delivery services.

10. Once Amazon caused the GateGuard device to be acquired by one of its channel partners, GateGuard activated the device. This meant that, when the device was sent to Amazon's secret laboratory, Amazon could observe how a connected device operates through its access to an activated device and could thus analyze the mechanisms by which the GateGuard mobile app conducts video conversations and unlocks doors. Amazon's software engineers could gain access to the GateGuard panel and observe how the panels and control system send a log of every entry attempt to GateGuard server technology on the cloud and could observe the functioning of this server technology itself.

11. GateGuard keeps the functioning of its system completely secret and only a highly developed research lab, such as the one at which the GateGuard device was analyzed, examined and ultimately copied, would have the tools and experience to gain access. On information and belief, the GateGuard device was taken to the locked laboratory room at Amazon's ultra-secret research center and later destroyed during the present litigation.

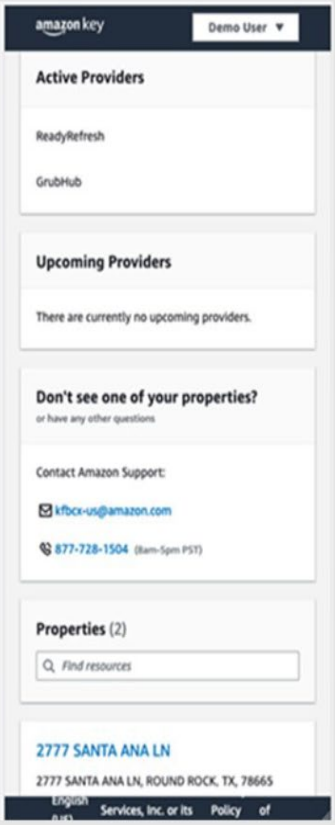
12. Moreover, at the time that Amazon misappropriated the GateGuard device, it was in

the process of testing the compatibility of intercom systems such as GateGuard's with the new Ring Intercom system it was developing for the European market and was introduced in 2022. See https://www.linkedin.com/in/kaushik-mani-970b57b/. In fact, Amazon was training employees and agents on the manner to integrate intercom systems such as GateGuard's with the Ring Intercom. On information and belief, the purpose of this "compatibility testing" and "training" was in fact to refine the features of the Ring Intercom to enhance its attractiveness and functionality, and to sharpen the integration of the Ring Intercom with existing intercom systems to facilitate market penetration for the Ring. Amazon was thus able to study and copy features of the GateGuard intercom that would add to the appeal of the Ring Intercom—without obtaining GateGuard's consent or compensating GateGuard, and then conveniently destroying the illegally obtained GateGuard device in the course of discovery. One of the people who identifies himself as the "lead inventor" of the Key for Business, Mr. Kaushik Mani, has publicly posted a video of the functioning of the Ring Intercom that incorporates elements of the GateGuard system. https://www.linkedin.com/feed/update/urn:li:activity:7084171069107941376/.

13. Property managers and tenants rely on GateGuard to keep their buildings safe.

14. GateGuard offers its devices and associated software on a subscription model based on a Service Agreement, pursuant to which GateGuard offers to install its intercom at a low upfront cost with recurring fees based on usage over a multiple-year period. GateGuard's Service Agreement is available at www.gateguard.xyz. The only way for customers to subscribe for GateGuard's products and services is through the www.gateguard.xyz website and the execution of the Company's Service Agreement.

15. In fact, after having examined the GateGuard system as a whole, Amazon is now rolling out a directly competing service through the Amazon Key. Amazon has announced to its channel partners the introduction of a new service based on its theft of GateGuard proprietary trade secrets:

2	Announcing the Launch of Property Management Portal for Property Managers	We are introducing a new web-based portal for property managers to manage third-party provider access with the release of the single signature install agreement. Once the property manager signs the install agreement and installation is completed at one of their properties, they will receive an email invitation containing the link to the property management portal within 1 month. Sales reps will also be provided with a test account to demonstrate the portal's functionality to interested property managers. Please refer to the following steps for more information.	

•

16. The above service closely parallels GateGuard's "Property Panel," the advantages of which GateGuard's founder, Ari Teman, specifically pitched to Amazon in October 2020. Amazon stated it was not interested in acquiring GateGuard—presumably because it would be easier to simply copy the Property Panel after it had illegally obtained one of GateGuard's devices through an alleged "client" of GateGuard. *See* ¶¶ 135-140s infra.

17. In addition, Amazon's subsidiary Ring rolled out a new video to phone message service, almost a carbon copy of the same, pre-existing GateGuard feature, in 2022, after Ring software engineers had evaluated the GateGuard system in 2021. *See* paragraph 10 above.

18. To place an order, a customer is required to confirm that it has read and agrees to the

Service Agreement and the related Terms and Conditions, which make clear, *inter alia*, that GateGuard is the owner of its devices. The relative rights and obligations of the Company and its subscribers are set forth in more detail in the section entitled, "The GateGuard Service Agreement and Terms and Conditions" below.

19. Amazon is not only destroying GateGuard's business by the conduct described above: It is compromising the safety of New York City residents – and *breaking the law*.

20. Specifically, N.Y. Multiple Dwelling Law § 50-a requires every apartment building in New York State be equipped with a working intercom system. The statute imposes ***criminal*** liability on anyone "who shall willfully destroy, damage, or jam or otherwise interfere with the proper operation of" such intercoms.

21. This is exactly what Amazon has done. At numerous buildings throughout New York City and in this District, Amazon installed its own devices without permission of building management and has destroyed, damaged, and interfered with the proper operation of GateGuard's intercoms either making the devices appear to be defective, or actually damaging the proper functioning of GateGuard's devices in order to return to the building and propose a security "upgrade" to unsuspecting property managers and owners who did not know of Amazon's initial installation.

22. Amazon has operated in a ruthless, cut-throat manner, pushing growth at all costs and signing up new buildings at breakneck speed, often without consent and by deceiving building superintendents that they have obtained management or ownership approval.

23. GateGuard has brought this issue to Amazon's attention repeatedly, even directly to its founder Jeff Bezos, starting in October 2020.

24. Yet Amazon refuses to take responsibility for its conduct or even to change its deceptive and unlawful practices, despite being on notice that its activities compromise the safety of building residents—including *Amazon's own customers.*

25. Moreover, GateGuard has now learned, as described above, that Amazon instructed its channel partner to pose as a GateGuard client and then subjected the GateGuard device and system as a whole to analysis at its top-secret research and development laboratory for purposes of developing a new competing property management tool and to refine its Ring Intercom system that it began to market in 2022 after Ring engineers had had the opportunity to examine the inner workings of the GateGuard system at its secret research laboratory.

26. Left with no other choice, GateGuard brings this suit to hold Amazon accountable for the damage it has caused, and to ensure that Amazon does not improperly profit from the proprietary technology it has accessed through its illegal conduct.

THE PARTIES

27. GateGuard, Inc. ("GateGuard" or "Plaintiff") is a Delaware corporation having a principal place of business at 1521 Alton Road, #888, Miami Beach, FL 331391. "GateGuard" is also Plaintiff's registered trademark.

28. Defendant Amazon.com, Inc. is a Delaware corporation having a principal place of business at 410 Terry Avenue North, Seattle, WA 98109.

29. Defendant Amazon.com Services, Inc., is a Delaware corporation having a principal place of business at 410 Terry Avenue North, Seattle, WA 98109.

30. Defendant Amazon.com Services, LLC, is a Delaware limited liability company having a principal place of business at 410 Terry Avenue North, Seattle, WA 98109.

31. Defendant Amazon Logistics, Inc. is a Washington State corporation having a principal place of business at 410 Terry Avenue North, Seattle, WA 98109.

32. Defendant Ring LLC is limited liability company with its corporate headquarters at 1523 26th Street Santa Monica, CA 90404 United States. Key for Business is a division of Ring and many of the Key for Business developers, including the "lead inventor" of the Key for Business, Kaushik Mani work for Ring on the development and introduction of Amazon's new Ring Intercom.

33. Upon information and belief, Defendants are and were at all relevant times the agents, affiliates, alter egos, partners, assignees, successors-in-interest, or principals of each other or were otherwise responsible for or participated in the performance of the wrongful acts alleged herein, and thereby are jointly and severally responsible for such acts and incurred liability therefore.

JURISDICTION AND VENUE

34. This court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338 in that this case arises under various federal statutes, including the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq., the Defend Trade Secrets Act of 2016, 18 U.S.C.A. § 1832 *et seq.*, the Lanham Act, 15 U.S.C. § 1125, the Sherman Antitrust Act of 1890, 15 USC § 2, and the Clayton Act of 1914, 15 U.S.C. § 12 *et seq*.

35. This Court has supplemental jurisdiction over all state law causes of action asserted herein pursuant to 28 U.S.C. § 1367, because Plaintiff's state law claims are part of the same case or controversy.

36. This Court has personal jurisdiction over Defendants because each of them conducts business in New York and because they have committed torts in the State of New York

and in this district.

37. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b), as a substantial part of the events, acts, omissions, and injuries giving rise to the claims occurred in this judicial district and because Defendants are subject to personal jurisdiction in this judicial district at the time this action has commenced.

FACTUAL BACKGROUND

General

38. Amazon has achieved market power in multiple segments of the Internet-based economy. After beginning as a lowly online bookstore, Amazon now controls 40% of the cloud storage market, 34% of the cloud hosting market, 33% of the cloud infrastructure services market, more than Microsoft, Google, IBM and Alibaba **combined**.[1]

39. Amazon's complete dominance of the overall e-commerce market is even more striking, as the chart below illustrates. Amazon has the power to dominate markets and is acting in an increasingly cutthroat manner that has attracted the attention of the Federal Trade Commission[2]

40. According to a recent report of the House of Representatives' Subcommittee on Antitrust, Commercial and Administrative Law, entitled Investigation of Digital Competition Markets (the "House Antitrust Report"), Amazon controls about 65% to 70% of all U.S. online

marketplace sales and is the most-visited website in the world for e-commerce and shopping. In a telling phrase, the House Antitrust Report defines Amazon as the "gatekeeper" for e-commerce, because third parties are virtually compelled to use the Amazon platform for e-commerce sales.

41. Amazon's most ambitious plan yet is to become the actual, and not merely metaphorical, gatekeeper for urban multi-family residences.

---

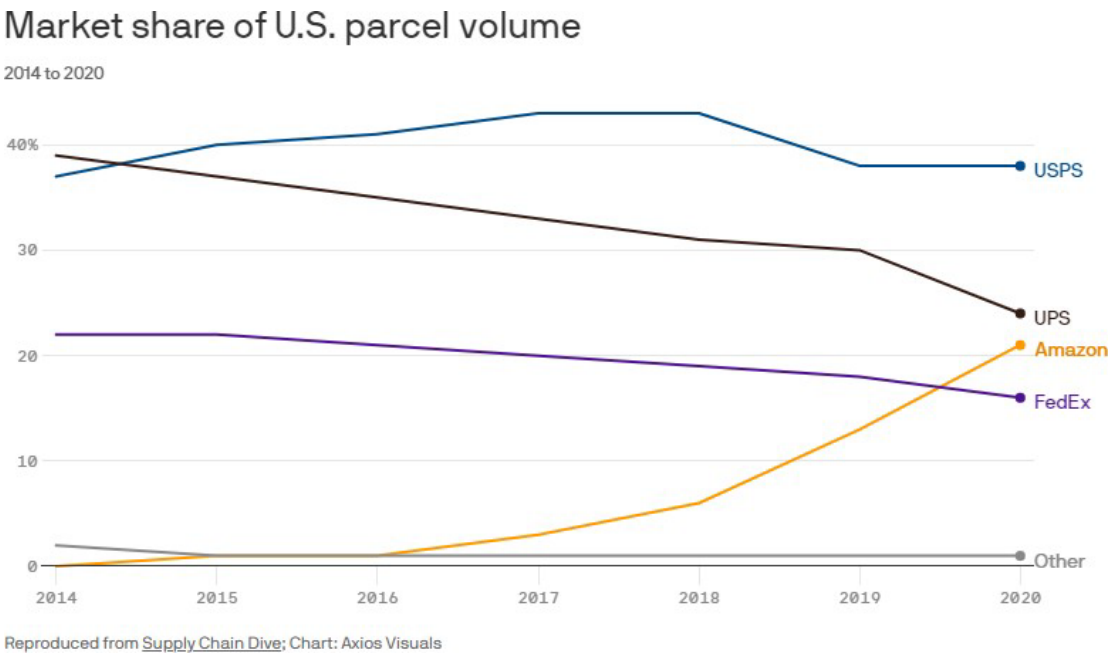
[1] *See* https://kinsta.com/aws-market-share.

[2] https://www.supplychainbrain.com/articles/30346-walmart-subsidizing-some-vendors-in-price-war-with-amazon (Amazon has also come under scrutiny for increasingly leaning on vendors to ensure that their products are not offered for a lower price on Walmart.com or any other rival website).

Amazon Logistics

42. Amazon's deliveries are effected through Amazon Logistics Inc., an Amazon subsidiary founded in 2016. In just a few short years, Amazon Logistics now controls over 20% of the **total package shipping market in the United States** and shows no sign of slowing down. Amazon Logistics' tremendous growth has vaulted it ahead of Federal Express, one of the industry leaders with decades more experience than Amazon logistics.[3] The charts below testify to the explosive growth of Amazon Logistics.

[3] https://www.asicentral.com/news/newsletters/promogram/october-2021/report-amazon-surpasses-fedex-in-us-shipping-share/



[4]

[4] https://www.asicentral.com/news/newsletters/promogram/october-2021/report-amazon-surpasses-fedex-in-us-shipping-share/

According to Axios, "Amazon has the potential to decimate UPS and Fed Ex."[5] Amazon's online platform is already undercutting the big players' average shipping rates by up to 33%, according to Freightwaves. As Axios puts it, Amazon's "tactic is a modern example of putting competition through a Rockefeller-style 'good sweating.'"[6]

32. Amazon already uses its market power to tie third party sellers on its "Amazon marketplace" platform to its fulfillment and delivery business. As the House Antitrust report puts it,

> Due to a lack of alternatives, third-party sellers have no choice but to purchase fulfillment services from Amazon. More than 73% of all Marketplace sellers worldwide reportedly rely on FBA services. Numerous third-party sellers told the Subcommittee that they feel they have no choice but to pay for FBA to maintain a favorable search result position, to reach Amazon's more than 112 million Prime members, and to win the Buy Box—through which the vast majority of Amazon sales are made. A recent consumer survey indicated that 75% of Amazon Prime customers specifically search for products flagged as Prime-eligible. As a result, as the Online Merchant's Guild told Subcommittee staff, many sellers will "say that without Prime you are dead."
> A competing online marketplace described how Amazon effectively forcing sellers into its FBA program makes it more difficult to compete with Amazon for sellers, stating, " [T]hrough anticompetitive strategies and practices by Amazon, many . . . sellers are being pulled into Amazon's tied marketplace-and-ecommerce-fulfilment ecosystem in a manner that makes them not only less independent but directly dependent on Amazon.

The Last-Mile Delivery Market

33. In 2016, the year Amazon Logistics was created, industry analyst Mordor Intelligence noted:

> The last mile delivery, being a final leg of logistics is very important, time consuming and also takes a major share in the overall delivery cost. Unlike the normal shipping, where large amount of cargo is transported along a fixed route, the last mile delivery

---

[5] https://www.axios.com/amazon-shipping-bigger-than-fedex-3dc5d80d-e16a-4531-9f45-1898a6261a78.html
[6] *Id.*

> involves transportation of goods in multiple routes with low parcel sizes. This cost has been vital for the retailers as the customers' expectations toward the fast and free delivery are growing. So, the companies and retailers are looking at advanced technological solutions and new delivery models to improve the overall process. According to various industrial estimates, the costs associated with the last miles stands around 50% of the overall logistics cost.

34. Historically, the private package delivery duopoly, UPS and Fed Ex, outsourced last-mile delivery to the US Postal Service ("USPS").[7] However, Amazon led the way in internalizing the last-mile delivery function, leading UPS and Fed Ex to follow suit.

35. E-commerce is the major driver of last-mile delivery growth. According to the US census, e-commerce sales for the second quarter of 2021, adjusted for seasonal variation, but not for price changes, was $222.5 billion. Unlike bricks and mortar retail sales, 100% of all e-commerce sales require last mile logistics delivery. While Amazon's share of total last mile delivery is not publicly available, if its share of the much larger national parcel delivery market has now surpassed Fed Ex and, likely, UPS, its last mile delivery market share must be even greater.

The E-commerce Delivery Market.

36. The total national e-commerce market was estimated at $767 billion in 2021.[8] The GDP of the New York Metro area was approximately $1.5 trillion before the onset of the Covid-19 pandemic[9] out of an approximately $21.5 trillion United States pre-pandemic GDP.[10] The New York metro area thus constitutes approximately 7% of US GDP and the New York e-

[7] https://www.savethepostoffice.com/postal-service-delivers-last-mile-almost-changing-modes-delivery/#:~:text=The%20Postal%20Service%20helps%20out%20FedEx%20and%20UPS,it%20does%20best%20%E2%80%9D%20%E2%80%94%20last%20mile%20delivery.
[8] https://www.statista.com/statistics/272391/us-retail-e-commerce-sales-forecast/
[9] https://www.statista.com/statistics/183815/gdp-of-the-new-york-metro-area/
[10] https://tradingeconomics.com/united-states/gdp

commerce market can be estimated at $53 billion. Monopolization of the e-commerce delivery market can be expected to increase Amazon's e-commerce market share 10% or more.

37. The e-commerce delivery market is booming.[11] The global e-commerce logistics market is estimated to generate $535 billion in annual revenues.[12] The US share of this market can be estimated at approximately $100 billion, of which approximately 60% is in transportation/delivery. *Id*. The size of the New York e-commerce delivery market can thus be estimated to be approximately $4 billion. While Amazon's immediate goal is to dominate e-commerce delivery so as to increase e-commerce retail sales, the harm to competitors can be measured as a contraction of the market share for Amazon's competitors, and either the disappearance of competitors or the conversion of competitors to clients.

38. Amazon already has market power in retail e-commerce, as the House Antitrust Report recognizes. Likewise, Amazon has market power over fulfillment logistics for third-party sellers who sell through the Amazon marketplace, as reflected in the 73% fulfillment rate for third party sales on the Amazon platform. If Amazon controls 70% of the online marketplace (with its own sales aggregated with third party sales) and its own sales amount to 50% of all online sales, this means that it must control in excess of 60% of all e-commerce deliveries.

[11] https://manometcurrent.com/e-commerce-in-parcel-delivery-market-is-booming-worldwide-with-lso-deutsche-post-fedex/
[12] https://www.alliedmarketresearch.com/e-commerce-logistics-market

39. Control of the ecommerce delivery market will feed back into and further reinforce Amazon's domination of the e-commerce market and position it to destroy other competitors as well or turn them into clients.

Residential Apartments and the Amazon "Key" to Control

40. In large urban environments, the vast majority of the population lives in multi-family apartments. In New York City, for example, 84% of the housing stock is in multi-family apartment buildings. https://furmancenter.org/thestoop/entry/report-growth-in-nycs-housing-stock-is-outpaced-by-growth-in-adult-populati.

41. All apartment buildings are required by law to have an intercom or access control system of some kind, and the intercom market in New York alone consists of hundreds of different companies. Just a few of these companies include Computer Integrated Services of New York, Advanced iCam New York, Intercom in NYC, Hillman Intercom, CBSIntercom Systems, Johnson Integrated Security Systems, United Security Systems, Easy Intercom, Parker Intercom Service and Brooklyn Intercom. Control of access to residential multi-family dwellings is the key to domination of the delivery market.

42. Amazon's strategy is not to displace all competitors in the access control market entirely—at least not immediately. Rather, its short-term aim is to position itself strategically in the access control space so as to monopolize the lucrative ***delivery*** market. In the longer term, on information and belief, Amazon also aims to use GateGuard's proprietary technology to develop a "smart" intercom of its own, displacing not only GateGuard entirely, but taking share from Google's Nest product.

43. In this e-commerce delivery market, Amazon's competitors are various entities of different types that provide package delivery services, and include the following:

- Third party-logistic ("3PL") providers such as Ship Bob and other fulfillment centers;[13]
- Other package delivery companies – UPS, Fed Ex, USPS, DHL that deliver directly or that work with e-commerce retailers or 3PL providers;
- Other e-commerce retailers that integrate their own delivery solutions or work with other package delivery companies;
- Building access providers with package delivery management functions such as GateGuard;
- Landlords who seek to control package delivery services, such as external storage, or partner with access providers such as GateGuard.

44. To gain a competitive advantage over all these competitors, in 2019, Amazon hit on the solution, which it calls the Amazon Key for Business, the "Key for Business" or "Key" for short.

45. The Key for Business is a small device that can be inserted into existing access devices or systems through an "extender" described in more detail below, or by being directly wired into an existing access system's wiring. The Key can remotely controlled and, once installed, Amazon deliverers can use it to obtain building access 24/7 without the intervention of any third parties, landlords or owners or access control devices.

46. All of Amazon's competitors in the e-commerce delivery market are threatened – and, as discussed below – damaged by the Amazon Key. The Key provides Amazon with a direct competitive edge over other package delivery services that do not have dedicated access to

[13] *See* https://www.shipbob.com/.

apartment buildings and thus have a higher cost structure (failed deliveries, circling time); over fulfillment services that similarly suffer from a pricing and reliability disadvantage; over delivery management companies that can be undercut and driven out of business as Amazon controls a larger and larger share of the market; and over landlords, who can no longer offer off-site storage as an economical alternative to immediate Amazon delivery. In short, the Key aims to be an ***essential facility***, through which a company that already controls 60-70% of the e-commerce delivery market can monopolize the market and, once competitors are driven out of business or turned into customers, raise prices on consumers with no alternative.

47. GateGuard GateGuard makes clear to its customers and potential investors that package delivery management is central to its business proposition, and a core element of its long-term value, as set forth in Section 13 of its Service Agreement:

> **13. PACKAGE AND DELIVERY MANAGEMENT**
>
> **1.** The goal of this system is to remove the burden and liability of package management from the management company, building officers, and staff, and to remove risks associated with package management. As such, GateGuard will have control over all aspects of package delivery, from who can deliver into the system, to when, and what.
> **2.** GateGuard may allow or disallow any delivery service, courier, or other organization or individual from accessing the service, or placing items into any package area. GateGuard may disallow any product or item into package area, such as but not limited to hazardous, oversized, or overweight items that may pose a risk to equipment and humans.
> **3.** GateGuard may require any or all Services to deliver to Holding Locations. This is for logistical reasons, such as to avoid overload, or traffic, or annoying residents at peak times, or excessive burden on the system or financials of the system. GateGuard may charge services a fee for usage of holding services. (Services will be able to deny this charge if they choose to hold the package themselves and re-deliver it at an approved time or return the package to its source).

48. The Amazon Key seeks to undermine and destroy GateGuard's separate package and delivery management services for Amazon products. The Key, pictured below, appears innocuous, but is in fact a competition killer.

49. The Amazon Key "brain" pictured above is wired directly into or onto the GateGuard circuitry, or the circuitry of other access control providers, often shorting the devices and/or their lock mechanisms due to polarity or voltage mismatches, as shown in more detail below. Critically, Amazon does not compete on the technological superiority of the Key device, which is a relatively "low-tech" and simple electronic "door key." Rather, to install its Key for Business, Amazon lies to building superintendents, claiming to have received authorization to

install its device when it has not received such consent, and then illegally tampers with already installed devices, such as the GateGuard intercoms, to place an "extender" inside the electronic devices belonging to others, including GateGuard, enabling Amazon to "piggy back" on the authorized access granted to parties such as GateGuard, bypassing landlords, property owners and other third-party access providers.

Key for Business is Designed so Amazon Can Dramatically and Cheaply Increase the Speed of its Deliveries, and Ultimately Control the E-Commerce Delivery Market .

50. Amazon's true motivations for deploying Key for Business are to control residential building access, thereby increasing the volume and speed of its deliveries to apartment buildings and becoming an essential service through which it can ultimately control the ecommerce delivery markets.

51. By installing its Key for Business within or on top of existing intercom/access control devices of third parties, Amazon can effectively control the e-commerce delivery market entirely. This is so because, with the priority, 24/7 access of the Amazon Key, Amazon deliveries can be made at any time, without the need to gain entry to the building from the customer, superintendent, or intercom/access controller. Other e-commerce retailers will not be able to compete with Amazon for delivery and will be forced to use Amazon's delivery service for a fee, thus making competitors customers.

52. Crucially, through the Key for Business, Amazon Logistics can obtain a decisive cost advantage over competitors. The chart below shows the magnitude of escalating cost issues for Amazon (and for all delivery companies).

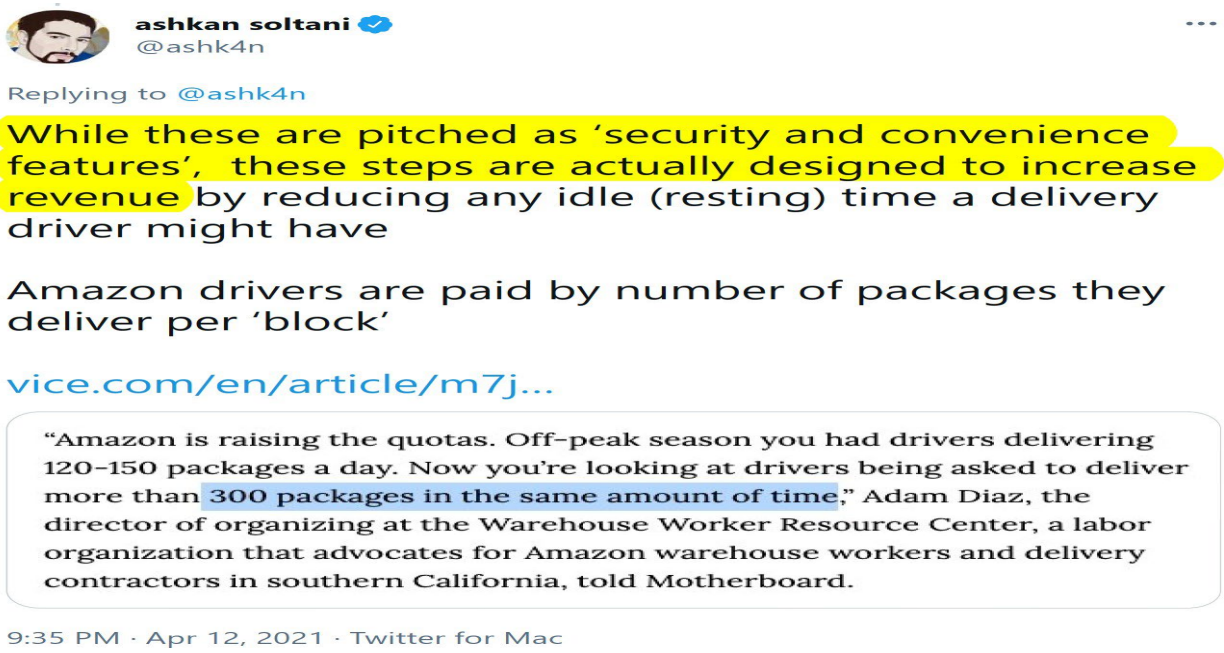
53. One of the main drivers of escalating costs in the congested urban environment is a lack of parking or extended standing places in the urban environment. Deliverers are forced to spend time and gas circling buildings, attempting multiple re-deliveries or cancelling deliveries altogether and incurring customer ill-will. With the Amazon Key, deliverers can offload and deliver to a common delivery area inside the residence multiple packages in minutes.

54. In addition, by ensuring more rapid, reliable deliveries through its Key, Amazon can market a faster, more efficient package delivery service not only for its own products, but also for third-party deliveries. E-commerce rivals will be unable to match Amazon for speed and reliability and will be forced to use Amazon for their deliveries. With total control of the delivery market, Amazon can engage in the other anti-competitive conduct identified by the House Antitrust Report: appropriation of third-party data, self-preferencing and extraction of anti-competitive user fees. Amazon can then create a "feedback" loop to further reinforce its

dominance of e-commerce retail, further enhancing its market power to dictate price at the expense of consumers.

55. With a built-out "Key" network, Amazon can offer its delivery service to Fed Ex, UPS and others as an unavoidable "last mile" delivery service, thus thwarting its competitors' services and forcing these competitors to become its own customers.

56. As a result of the foregoing, ***Amazon has been able to double the delivery quotas imposed on its drivers***, increasing the volume of deliveries from 125-150 packages a day to 300 packages in the same time period, as documented by one well-informed commentator:



57. As bad as the conduct by Amazon alleged above was prior to 2020, it got worse when ecommerce activity increased during the COVID-19 pandemic, as Amazon saw an opportunity to monopolize the e-commerce delivery market. Much as Amazon cloud services have become central to the Internet in such a way that natural competitors are compelled to turn to Amazon rather than develop rival technology, Amazon's aim is to develop its delivery system so

extensively that rivals will find it cheaper to turn to Amazon Logistics for their deliveries than to ensure such deliveries on their own.[14]

58. With a built-out access control network, Amazon can also offer its delivery service to Fed Ex, UPS and others as an unavoidable "last mile" delivery service, thus cannibalizing its competitors' services while simultaneously forcing these competitors to become its own customers. Amazon's ubiquitous vans and trucks provide a vivid illustration of Amazon's dominant and growing power.

Amazon's Patterns of Lies and Deception About its Key for Business

59. In its press release announcing the Key for Business,[15] Amazon claimed that its Key for Business "allows building owners and managers to give controlled access to delivery drivers to drop off Amazon packages to their residents[.]" This press release was materially false when made because Amazon intended from the outset to bypass the property owners and deceive superintendents and managers, tricking them into believing no owner or third-party consent was necessary.

60. In an attempt to shield itself from legal liability, Amazon has built a network of partners who approach and sign up "customers" for its Key for Business devices. Because the Amazon Key is "sold" for free, the partners responsible for directly marketing the Amazon Key can only be **profitable by** ensuring a huge volume of installations. This incentivizes the partners to engage in a wide variety of shady practices, including forging signatures on installation agreements, losing installation agreement, failing to use installation agreements, presenting themselves to superintendents as authorized representatives who have already been approved for installation, falsely reporting "authorized" personnel at building locations, using fictitious email addresses that are never checked, and submitting documents to Amazon designed to paper their fraudulent conduct

but that Amazon knows or should know perfectly well do not correspond to a genuine acceptance of the Amazon Key by an authorized building representative. The Amazon Key not only interferes with the functioning of existing intercom systems, thus preventing the functioning of the magnetic "door strike" that permits access to buildings, but the Amazon Key also deprives property owners and package management services of the right to control and charge a fee for access to their building. Amazon's "free" device is actually subsidized by the property owners and package delivery companies who never learn that the Amazon Key has been installed until there is a problem with the functioning of the existing intercom system, if at all.

---

[14] Media reports document that Amazon's efforts have come at the expense of the health and safety of these drivers. Lauren Kaori Gurley, *Amazon Delivery Drivers Are Overwhelmed and Overworked by Covid-19 Surge*, Motherboard (July 1, 2020) https://www.vice.com/en/article/m7j7mb/amazon-delivery-drivers-are-overwhelmed-and-overworked-by-covid-19-surge (documenting how Amazon's "punishing culture" and "skyrocketing quotas" "made conditions for Amazon's roughly 75,000 delivery drivers grueling and dangerous" including by forcing drivers to violate traffic and safety laws and forego lunch and bathroom breaks to meet Amazon's expectations). *See also* Patricia Callahan, *Amazon Pushes Fast Shipping but Avoids Responsibility for the Human Cost*, N.Y. Times (Sept. 5, 2019) https://www.nytimes.com/2019/09/05/us/amazon-delivery-drivers-accidents.html (documenting how Amazon's "relentless push for e-commerce dominance" pressures its drivers into unsafe situations, but when accidents result, Amazon goes to great lengths to "shields itself from liability").

[15] https://press.aboutamazon.com/news-releases/news-release-details/key-amazon-introduces-new-products-and-services-expand-its (last accessed April 15, 2021).

61. Promotional materials further the sales pitch that "Amazon Key for Business is completely free and perfect for apartments, gated communities, and office buildings. . . Amazon Key for Business (KFB) connects with a smart fob to let building owners and managers safely & seamlessly grant access to Amazon's fully vetted and tracked delivery drivers."

62. Amazon's website[16] claims that Key for Business "works seamlessly with" and "does not disrupt the existing building access system." Amazon repeats the same claims in direct communications with prospective customers.

63. These claims are false.

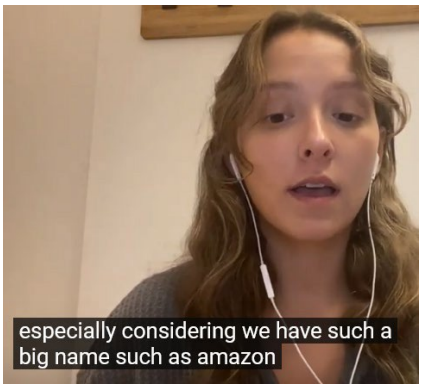
64. Amazon knows these claims are false.

65. A recently posted video provides further insight into Amazon's sales tactics:

KFB Sales Pitch Example

[16] https://www.amazon.com/b?ie=UTF8&node=18530497011 (last visited April 11, 2021).

66. In this video,[17] an individual identified as one of Amazon's "Regional Directors" explains how Amazon's sales representatives promoting KfB to building owners can leverage Amazon's prominence to gain the trust of business owners ("Amazon is a very respected business" with "such a big name").



67. In the video, ***Amazon sales reps are explicitly encouraged to keep their pitch as "simple" as possible so that potential targets – low level managers and superintendents – do not "get nervous" and can be tricked into signing a contract with Amazon without "feel[ing] the need" to contact "a higher up***."

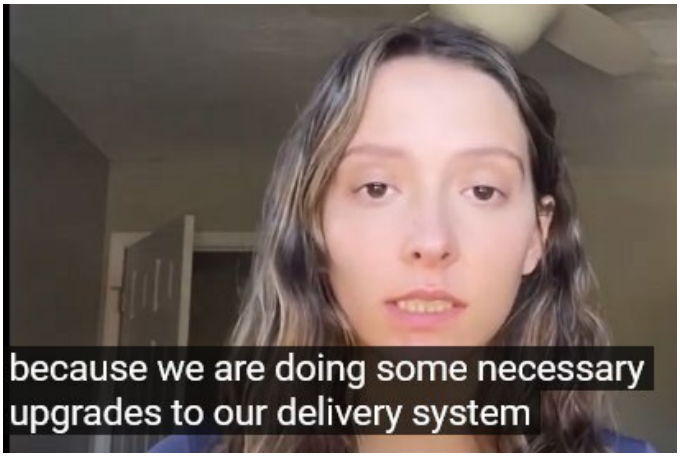
68. Amazon also uses deceptive language to promote its Key for Business.

69. In written and verbal communications with prospective customers, Amazon is

[17] https://www.youtube.com/watch?v=jpD20m4d_mE (last visited April 14, 2021).

careful to characterize Key for Business as an "update" or a "necessary upgrade to [Amazon's] delivery system."

70. For example, the above-referenced video documents how Amazon describes KfB to building owners as a "necessary upgrade[] to [Amazon's] delivery system:"



71. This is of course a complete lie as Amazon is not updating or upgrading any of its own delivery devices, but is interfering with, and attempting to override, the existing access devices already installed at the gate.

72. Amazon uses this deceptive language knowing few consumers will question or forgo an "update" or "upgrade" Amazon says is "necessary."

73. In the promotional materials attached to this email Amazon insists that Key For Business is simply an update and "procedural fix," even though it does not actually update any Amazon products.

74. Amazon also lies in its promotional materials that its product will not interfere with existing commercial access methods, deliberately pretending it will seek business owner consent for installing its devices and conflating residents' access with the access control of third-parties controlling commercial including GateGuard, other intercom providers or the property managers

or business owners themselves:

> Amazon Key for Business is a new security update and procedural fix for delivering packages to multi-family buildings. Amazon will now use AWS cloud technology to track our packages and track our delivery drivers. Building owners and managers who participate in the update, will use this same cloud technology to control access of Amazon delivery drivers and create specific package delivery instructions for your building.
>
> **Q: Will Key for Business change the existing access experience for my residents?**
>
> A: Your residents can continue to use their existing access methods. Key for Business does not disrupt the existing building access system.

The Superintendent Bypass Strategy

75. In reality, as described above, Amazon sales reps are specifically instructed to make the sale with lower-level individuals, such as a superintendent, without seeking the consent of "higher ups," *i.e.*, the landlord or property manager.

76. Amazon partners routinely target the superintendents of buildings, some of whom do not speak English, and either forge the superintendents' signatures, provide fake marks of assent, or install without any agreement at all after conning an unsuspecting superintendent into believing the Amazon Key has already been approved for installation, and use an unsuspecting superintendent's agreement as license to install the Key on dozens if not hundreds of portfolio properties around New York City.

77. Amason is fully aware of the superintendent bypass strategy and either turns a blind eye to the obvious red flags in the documentation and reporting of alleged transactions with unsuspecting superintendents or actively condones the superintendent bypass strategy, because the overarching aim of the Amazon Key is to dominate the package delivery market as quickly as possible.

Amazon Falsely Claims Key for Business "Does Not Disrupt" Intercoms

78. In promotional materials and other documents used to promote Key for Business to consumers, Amazon falsely claims its device can be added to any existing "control system" in a "secure" manner, deliberately concealing the fact that its device interferes with and is used to disable third-party control systems.

Can the device be physically hacked and allow intruders into my apartment building?

Installing Key for Business to any control system you have is completely secure. The device is designed to prevent physical hacking

Building Access Controller FAQs – Security and Control

key for business

- How secure is installing another access control device in my building? Can it be physically hacked and allow intruders into my apartment building?
  - Installing "Building Access Controller" to any control system you have is completely secure. The device is designed to prevent physical hacking.

79. On its website,[18] Amazon claims that Key for Business "works seamlessly with" and "does not disrupt the existing building access system."

5. Will Key for Business change the existing access experience for my residents?

Your residents can continue to use their existing access methods. Key for Business does not disrupt the existing building access system.

80. These claims are false.

81. Far from "completely secure," Amazon's Key for Business *itself* is a serious security risk for buildings. In many instances, Amazon's Key for Business installations interfere with or destroy a building's primary intercom, electric door locks, and other components.

82. Contrary to Amazon's representations, by disabling or destroying the building's primary access system, Key for Business plainly *does* "allow intruders into. . . apartment building[s]" since the device is designed to perform one function and one function only: ensure that Amazon drivers can make deliveries into buildings without resident, superintendent, property manager or third-party control or approval.

Amazon's Relentless Hounding of Potential Customers

83. In addition to its deceptive sales tactics, Amazon is relentless in pushing the installation of Key for Business. Customers report that Amazon's representatives hound them incessantly (by phone, email, and in person)[19]:

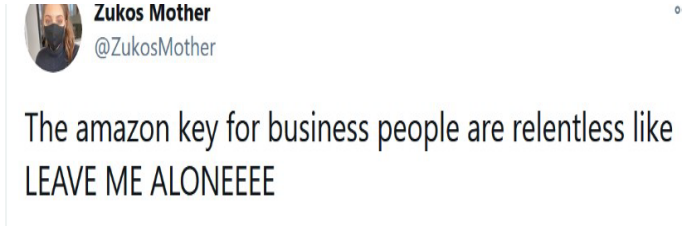
---

[18] https://www.amazon.com/b?ie=UTF8&node=18530497011 (last visited April 11, 2021).

[19] *See, e.g.*, https://www.multifamilyinsiders.com/apartment-ideas/the-front-lines/17596-all-i-want-for-christmas-is-to-be-off-of-the-amazon-key-call-list (last accessed April 15, 2021), including reports such as:

- "They're relentless!!"
- "I'm about to get a restraining order."
- "Omg. They are THE WORST. I can't be more clear at this point and they continue to call. It is so annoying and disruptive."

See also https://www.multifamilyinsiders.com/apartment-ideas/the-front-lines/18024-any-communities-out-there-using-amazon-key-for-business-pros-cons (last accessed April 15, 2021):



Amazon Ignores Management's Instructions and Installs Key for Business Without Consent

84. Unsurprisingly, Amazon's hard-ball sales tactics have been successful. Occasionally, if they have been approached at all (when the classic superintendent bypass strategy has not been adopted)property managers begrudgingly relent and allow Amazon to install Key for Business, taken in by Amazon's lies that the device will not interfere with its existing access control system.

85. Often, however, a firm "*no*" does not stop Amazon. When their aggressive tactics fail, Amazon sales reps proceed to the location and install Key for Business anyway – ***<u>without</u>*** *the property owner's consent.*[20] To avoid the consent of management entirely, Amazon reps are instructed to seek out and pressure lower-level employees to close a deal quickly so the nervous

- "They pressured us to get installed quickly, but none of the drivers even know what it is…. I think it's all a scam[.]"
- "Not only did nothing change but everyday we get solicited by Amazon and asked if we want this service that we already have…. [O]ur deliveries with them have gotten worse if that is possible."

[20] https://www.multifamilyinsiders.com/apartment-ideas/the-front-lines/18024-any-communities-out-there-using-amazon-key-for-business-pros-cons (last visited April 11, 2021).

employees will not contact "higher-ups."

Any communities out there using Amazon Key For Business? Pros? Cons? 2 weeks 1 day ago

Tweet Amazon has been to my property numerous times attempting to sell me on Amazon Key and I kept telling them no as we have always opened our gate for delivery drivers as soon as we see them pull in. One day, our gate malfunctioned. When our control access vendor came out to look, they noticed an Amazon box was installed (Amazon Key) in our control panel. When they installed it, they ripped out a main wire which was pricey to replace. After numerous calls to Amazon, I'm still trying to get reimbursed.
The fact they did this has rubbed me the wrong way entirely as this was done without consent.

86. Based on the number of social media posts discussing this phenomenon, it is reasonable to infer that Amazon is systematically installing its Key for Business devices without consent.

GateGuard's Devices, Service Agreement and Terms and Conditions.

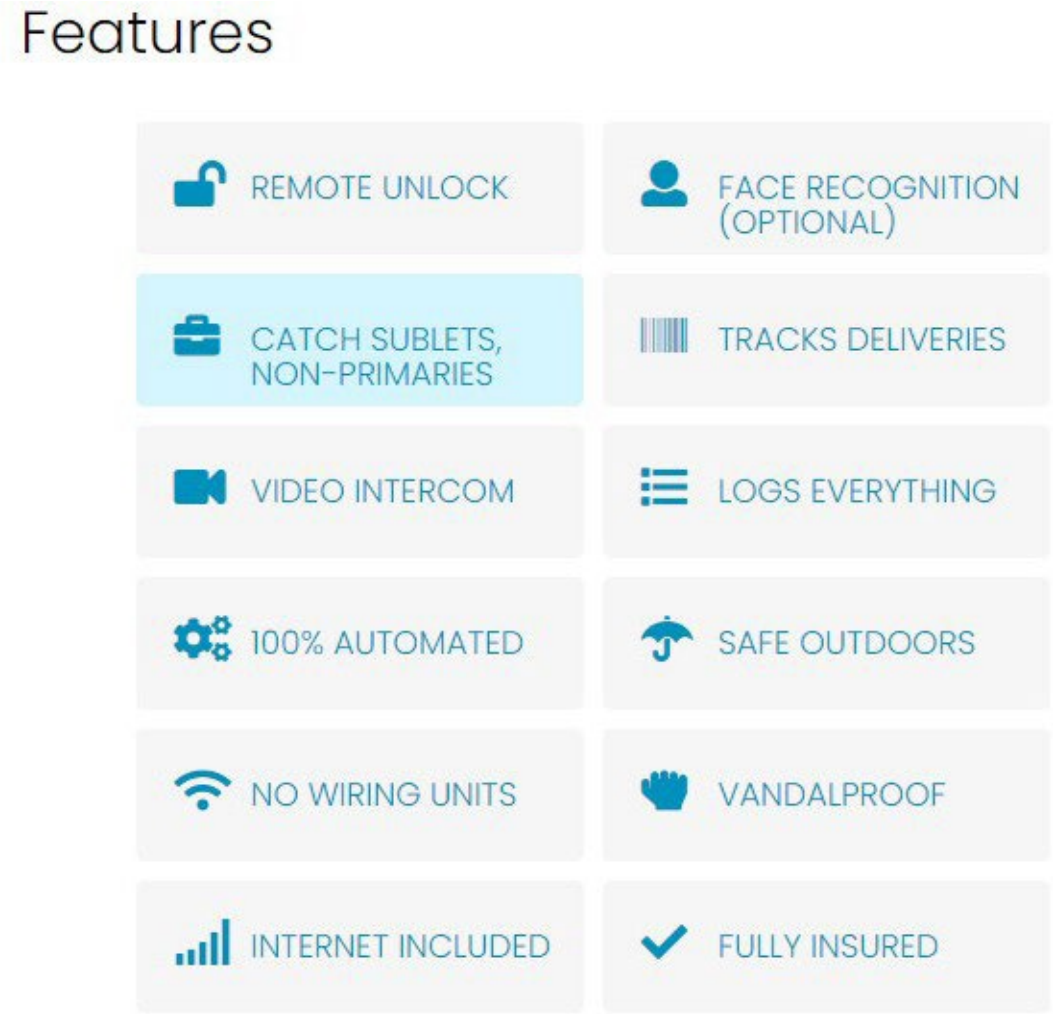
87. GateGuard's flagship device is an Android OS-powered intercom with face detection and recognition capability, cloud interaction and storage, video chat, 4G LTE connectivity, a router for providing wired and WiFi connectivity, NFC connectivity, data storage, and more. The device is seamlessly integrated with a website that permits landlords and property owners to track activity and usage, providing an online log of each entrance into the building and enabling clients to monitor non-primary uses, illegal sublets and the entrance of large groups. *See* https://youtu.be/Ski0UqQZKEU. Use of the Company's website is governed by GateGuard's Terms and Conditions that reinforce the Company's proprietary rights in its devices, intellectual property, and website. *See* https://gateguard.xyz/legal/terms.php.

88. The GateGuard AI Intercom is built around proprietary technology that includes the configuration of its motherboard, the placement and type of electronic circuitry and other components used, the insulation resistance between circuits, the voltages at which the device operates, the mechanisms of internet connectivity and the antennae used. In addition, the inner casing of the intercom, its system of wall-mounting and hinges, its waterproofing design and its

custom-designed cables are all proprietary to GateGuard and kept secret from competitors and customers, with only authorized GateGuard agents permitted access to the devices for repairs and troubleshooting. By breaking into the GateGuard "box," a competitor such as Amazon is able to steal or damage such proprietary technology. On information and belief, Amazon is using GateGuard's proprietary technology to develop certain Key functionalities and to develop a smart intercom of its own that will enable it to enter the smart building access control market and compete not only with GateGuard, but also with devices such as the Google Nest.

89. Amazon's playbook in stealing technology from early-stage companies is well-established. *See* https://www.wsj.com/articles/amazon-tech-startup-echo-bezos-alexa-investment-fund-11595520249. In one well-documented episode, Amazon obtained access to the financials, strategic plans and other proprietary information of a company called Nucleus, and then developed an Alexa-enabled video chat device, called the Echo Show, that performed many of the same function as Nucleus' device, leaving the Nucleus founders and other investors "furious" as "there was no way [the] small company could compete against Amazon in the consumer space." *Id.*

90. The functionality of the GateGuard flagship device is shown below:



91. Amazon's aggressive build-out of its Key network runs headlong into companies such as GateGuard that have proprietary rights in the devices Amazon needs to exploit for its strategy to be effective. The Amazon Key is wired directly into a building's existing intercom system to give its deliverers direct access to the apartment lobby and to mask Amazon's use and misuse of existing installations.

92. GateGuard protects its proprietary rights in its devices through a Service Agreement and its Terms and Conditions that must be accepted by all GateGuard customers without

exception.[21] The Company customer acquisition model, contractual relationships and legal rights are spelled out in detail on the Company's website, www.gateguard.xyz. It is impossible to become a GateGuard customer without acknowledging the Company's Service Agreement and Terms and Conditions through the Company website.

93. The Service Agreement makes clear the GateGuard customer is a "subscriber," not the owner of GateGuard installations. See Service Agreement, https://gateguard.xyz/legal/serviceagreement.php. Customers are required to provide a Maintenance Security Deposit for the installation of a GateGuard device. *Id.* The manufacturer's suggested retail purchase price for a GateGuard device is $8649. Rather than selling the device, however, the Company leases its devices to the customer for a heavily discounted product fee of $3699 plus the Maintenance Security Deposit. *Id.*

94. In addition, the Company provides a "non-exclusive, non-transferable license, without the right to sublicense, to run the Product Software as incorporated into the Products during the Term solely for Subscriber's use of the Product in conjunction with any Services ordered" under the Service Agreement. *Id.* The base Subscription Fees include up to 1 GB of cellular data usage per month. Subscribers can either pay monthly fees on a sliding scale determined by the length of the contract or can prepay the total contract fees to achieve maximum savings. *Id.*

95. Upon early termination of the subscription contract, the full retail cost of the device is due, much like an auto lease, where the early termination of a leased vehicle results in a charge for the full purchase price. The customer also pays a service termination fee on early termination.

[21] Early in the Company's history, in 2017 and 2018, a handful of customers claimed, in bad faith, that they were unaware of the Company's Terms and Conditions and that they had somehow purchased devices directly from the Company without using the Company's website.

96. As a reflection of GateGuard's ownership rights, the Service Agreement states that GateGuard makes "an intense effort to protect *our devices*, networks, connections, and data" (emphasis added) and provides an indemnity for GateGuard's customers against any third-party claims that the GateGuard products or services infringe any validly registered U.S. patent, copyright or trademark.

97. Customers are also required to acknowledge the Company's privacy agreement, which reflects GateGuard's commitment to protecting the privacy rights of its customers and device users, while underscoring the Company's proprietary rights, clearly expressed as follows: "We collect information from you when you register on our site, of via *our devices*, login via our apps, place an order, subscribe to a newsletter, respond to a survey, fill out a form, Use Live Chat, Open a Support Ticket, use our devices, or enter information on our site or devices or apps." *See* https://gateguard.xyz/legal/privacy.php (emphasis added).

GateGuard's Falls Prey to Amazon's Ruthless Tactics

98. On information and belief, Amazon has installed its Key for Business devices at over 40 buildings where GateGuard was already installed, either without the property owner's consent or by misrepresenting the effect the Amazon device would have on the GateGuard intercoms and resulting in the malfunctioning of GateGuard equipment, customer complaints, loss of revenue and loss of goodwill. Where the Amazon Key has not caused malfunctioning, Amazon has been able to free ride on the GateGuard device, without paying a royalty or usage fee, because its conduct is secretive, hidden and deceptive.

100. The consequences of Amazon's conduct have been devasting to GateGuard. The company has lost contracts covering over 110 buildings as a result of Amazon's tactics. When a

device malfunctions at one building as a result of Amazon's actions, GateGuard loses the entire

portfolio of buildings operated by a single manager. Thus, Amazon's conduct has a devastating multiplier effect on GateGuard's business, resulting in millions of dollars in lost revenues. In addition, where the Key has not caused malfunctioning, Amazon has been able to profit illicitly from GateGuard's brand and devices. At none of these buildings did GateGuard authorize the installation of Amazon's Key for Business into its own devices and, on information and belief, none of the installations were authorized or authorized with full disclosure. There are likely hundreds of additional buildings illegally using the Amazon Key without GateGuard's knowledge or consent.

101. Property managers have blamed GateGuard, rather than Amazon, for malfunctioning or service interruptions resulting from the Amazon Key's surreptitious installation of the Key, not knowing the full story and not considering the possibility that Amazon would operate in the ruthless and anti-competitive manner discussed herein. This has damaged GateGuard directly in its earnings as well as falsely damaged GateGuard technology's reputation in the industry.

102. As noted, Amazon achieves these unauthorized installations by arriving at a building and (falsely) representing to unwitting residents or building personnel that the building's management has authorized Amazon to install Key for Business. This strategy has been documented over and over, as indicated below:

Amazon Key 4 Business

Last Monday, a couple guys buzzed my apartment saying they were from "Amazon Key." I came downstairs to the front of my building. One guy showed me a lanyard with the Amazon logo and said that they're hear because we've had reports of stolen packages (which is actually true) and they'd like to install an Amazon Key device in my buzzer to allow Amazon drivers access to our building. I asked if they'd spoken to my landlord, and they claimed that they had, he was okay with this (they had his name written down on their iPad) and they just needed someone on site to authorize this. It felt fishy, but I guess because of a momentary lack of judgement or pressure, I went ahead and scheduled the appointment for the next Monday.

After the appointment I texted some friends and Googled this, and came across this article, which sounded similar to my experience. My friends also said it sounded sketchy.

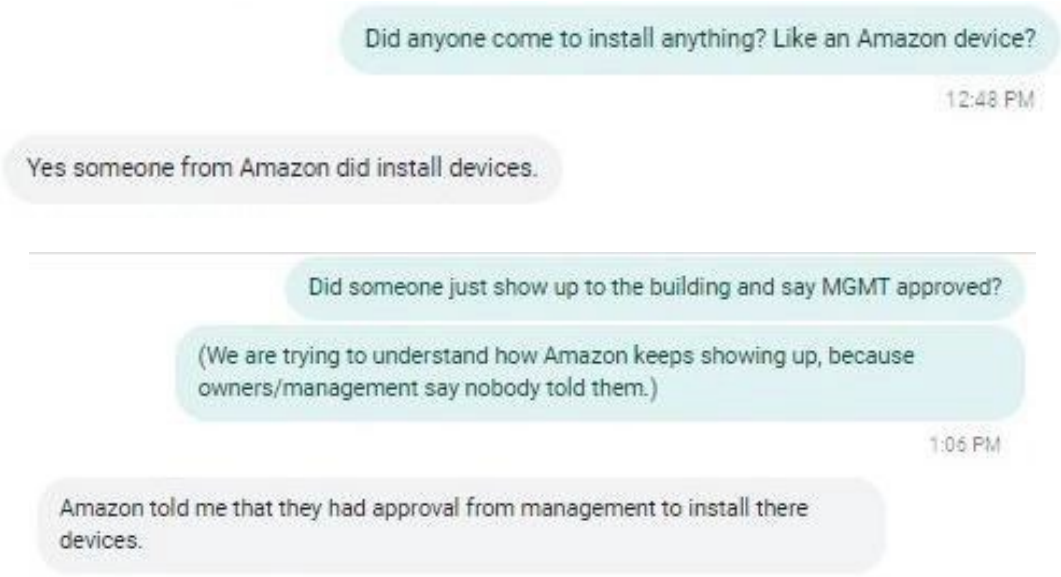
https://www.10news.com/news/local-news/new-scam-targets-local-amazon-customers-worried-about-package-thefts

I called the phone number on my confirmation email (which was from "noreply@amazonkey4business.com", another flag) and a not-so-professional-sounding Rep answered the phone. I asked to cancel and for a confirmation email. The rep agreed, but I never received a confirmation email. I then emailed my landlord and my landlord said that someone had contacted him, but he never authorized anything and didn't want this set up.

103. When representatives of one of the world's largest and best-known companies represent that they have secured authorization to install equipment, it is little surprise that building personnel and tenants often trust these representations and allow Amazon to install Key for Business.

104. Amazon has followed this same "playbook" to install Key for Business at least forty buildings that utilize GateGuard's intercoms, without authorization and in a manner that intentionally or recklessly damages GateGuard's devices. The damage to GateGuard's business has a multiplier effect, as landlords who have been deceived into believing GateGuard malfunctions at one building cancel contracts covering dozens of additional buildings throughout Manhattan.

105. This is not conjecture. GateGuard has specific proof that Amazon lies to building superintendents to install Key for Business inside the GateGuard intercom, as evidenced in the following dialogue between a GateGuard representative and a building superintendent:



106. GateGuard contacted building management who confirmed they had *not* authorized Amazon's installation:

From: [redacted]>
Date: Wed, Oct 21, 2020 at 12:54 PM
Subject: Re: [redacted] & [redacted] West [redacted] Street
To: [redacted]>
Cc: [redacted] <[redacted]>, [redacted] [redacted]>

I didn't authorize anything from Amazon. No one ever contacted me for anything from them.

107. Not only was the installation of Key for Business unauthorized by building management, it was ***never*** discussed with ***GateGuard,*** which, under its contract, has ***exclusive*** control over package management and access control devices on each building where it is installed. Amazon knows GateGuard has an agreement with the property manager for operation of its intercom and, as a sophisticated market participant, knows that no intercom provider would agree to allow another company to install their equipment on top of its own without consent and thus

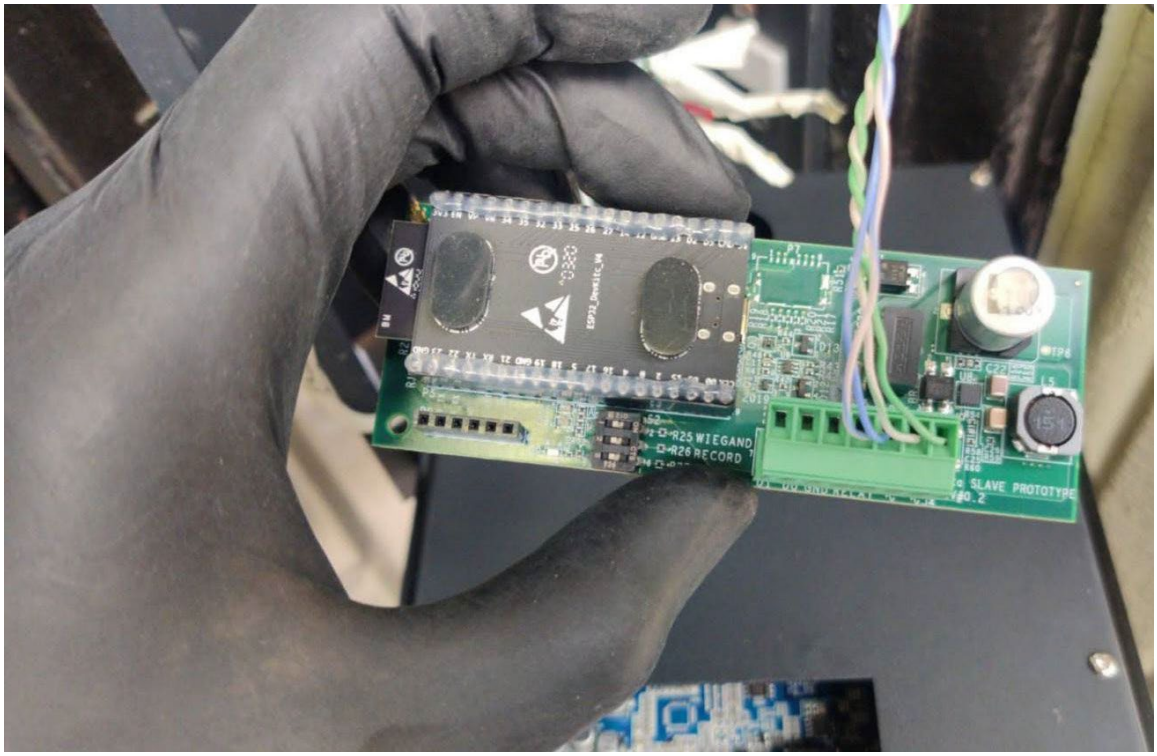
knows that it is intentionally interfering with GateGuards contractual relations with the property owners.

108. Generally, GateGuard only learned of the installation after the client complained that the intercom – which had had no problems prior to the surreptitious insertion of the Key for Business into Gateguard's device – was now malfunctioning, leaving it with no effective remedy other than to demand damages from Amazon, which Amazon refuses to pay. If Amazon's illegal use does not cause device malfunctioning, GateGuard has no effective means of catching every instance of Amazon's unauthorized conduct, resulting in unearned profits for Amazon.

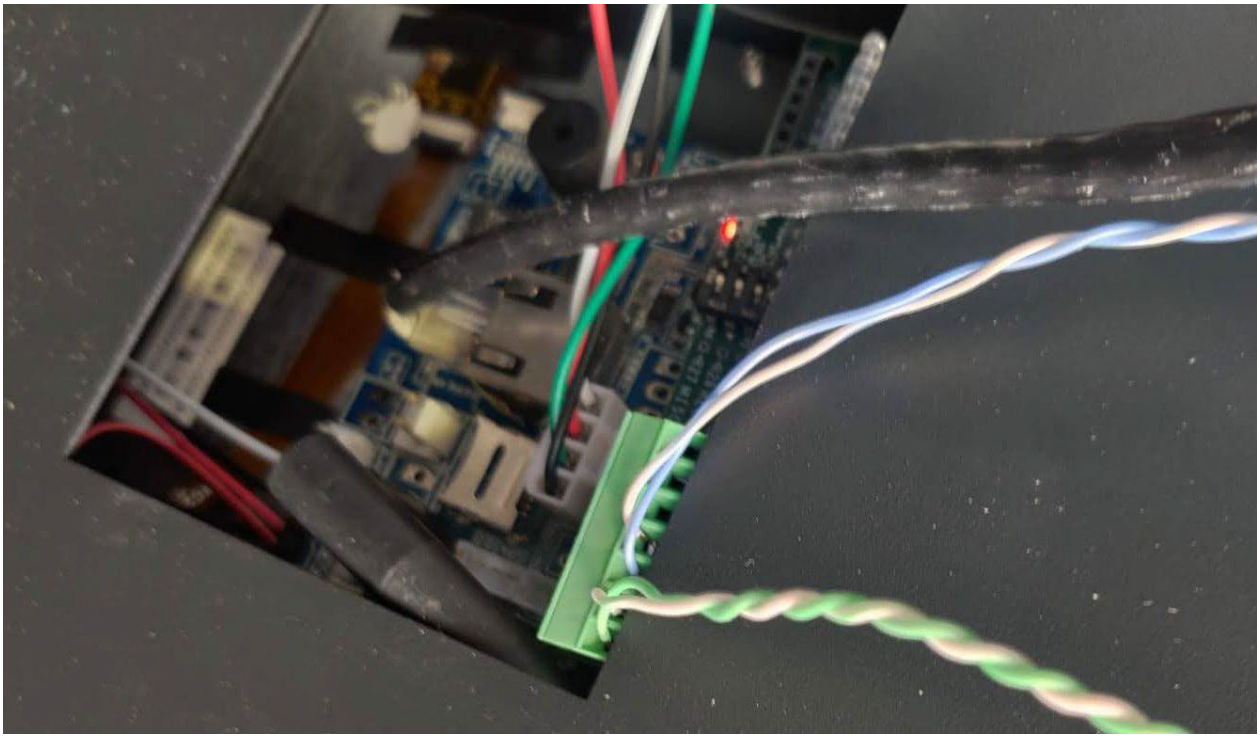
109. The reason that Amazon's Key for Business can be so damaging to GateGuard's intercom is that the Amazon device is installed directly onto the GateGuard circuit board or wiring that is connected directly to the circuit board, often "shorting" the devices and rendering them inoperable.

110. Even though Amazon operates in great secrecy, GateGuard has been able to catch Amazon "red-handed" tampering with its intercom device.

111. The image immediately below shows Amazon's extender, a subway-ticket size device that needs to be inserted in or connected to an existing intercom or access control system:



112. At one building in Manhattan, GateGuard discovered this "extender" device inserted and connected inside GateGuard's intercom. The picture shown below is the back of a portion GateGuard's intercom. The extender device has been wedged onto Gateguard's blue circuit board; the green strip connecting the extender wires to a separate Amazon device can be seen on the bottom right and the grey "bubbles" that can be seen on the upper left-hand portion of the extender depicted above can be seen on the upper right-hand side of GateGuard's case below:



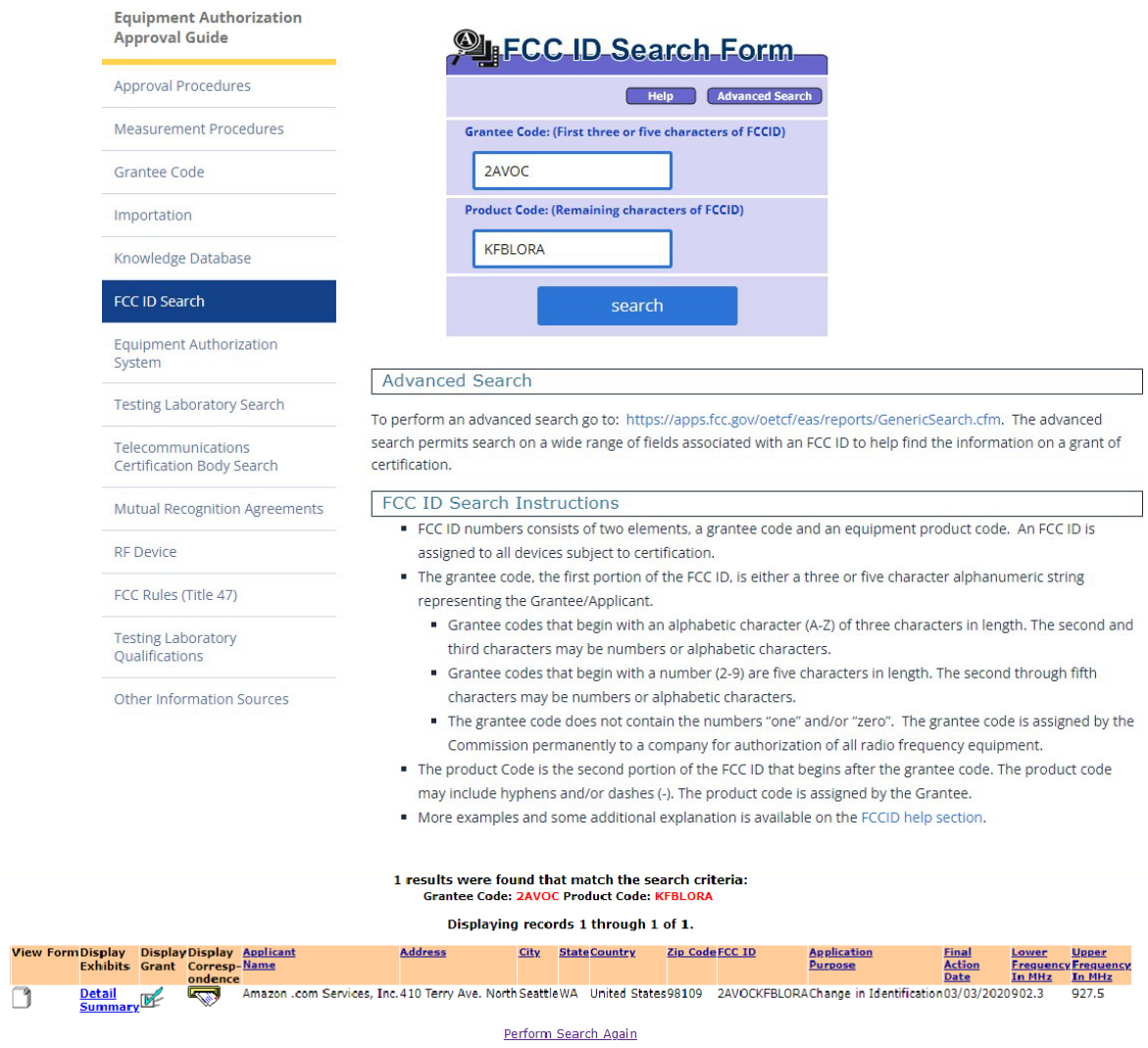
113. By connecting its device into the GateGuard intercom, Amazon can illegally "free-ride" off of GateGuard's product while being placed on or near GateGuard's circuitry resulting in malfunctioning that is blamed on GateGuard.

114. The dangerous placement of Amazon's unauthorized device can be clearly seen in paragraphs 108 and 109. Circuit boards are incredible delicate electronics which are protected by cases and should not have even the tiniest unauthorized objects – let alone an entire alien circuit board – pressed against them. The insertion of the smallest objects on top of a circuit board cause an electric short, a broken part, or other permanent injury to the board. In this case, by wedging its "extender" into GateGuard's case, Amazon damaged GateGuard electronic components, irreparably destroying the intercom screen.

113. The "extension" benefits Amazon when the device does not malfunction and harms GateGuard when it does, by shorting its device, damaging the intercom screen, and disabling other electronic components.

114. The "extender" is clearly connected to the Amazon Key for Business device, as shown by the sticker on the reverse of the device identifying the model name, number and FCC ID, as well as the amazon.com website specifying ownership of the product.

115. The FCC ID clearly identifies Amazon.com Services Inc. as the "applicant/grantee", as shown below:



Equipment Authorization Approval Guide

- Approval Procedures
- Measurement Procedures
- Grantee Code
- Importation
- Knowledge Database
- FCC ID Search
- Equipment Authorization System
- Testing Laboratory Search
- Telecommunications Certification Body Search
- Mutual Recognition Agreements
- RF Device
- FCC Rules (Title 47)
- Testing Laboratory Qualifications
- Other Information Sources

FCC ID Search Form

Help | Advanced Search

Grantee Code: (First three or five characters of FCCID)

2AVOC

Product Code: (Remaining characters of FCCID)

KFBLORA

search

Advanced Search

To perform an advanced search go to: https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm. The advanced search permits search on a wide range of fields associated with an FCC ID to help find the information on a grant of certification.

FCC ID Search Instructions

- FCC ID numbers consists of two elements, a grantee code and an equipment product code. An FCC ID is assigned to all devices subject to certification.
- The grantee code, the first portion of the FCC ID, is either a three or five character alphanumeric string representing the Grantee/Applicant.
  - Grantee codes that begin with an alphabetic character (A-Z) of three characters in length. The second and third characters may be numbers or alphabetic characters.
  - Grantee codes that begin with a number (2-9) are five characters in length. The second through fifth characters may be numbers or alphabetic characters.
  - The grantee code does not contain the numbers "one" and/or "zero". The grantee code is assigned by the Commission permanently to a company for authorization of all radio frequency equipment.
- The product Code is the second portion of the FCC ID that begins after the grantee code. The product code may include hyphens and/or dashes (-). The product code is assigned by the Grantee.
- More examples and some additional explanation is available on the FCCID help section.

1 results were found that match the search criteria:
Grantee Code: 2AVOC Product Code: KFBLORA

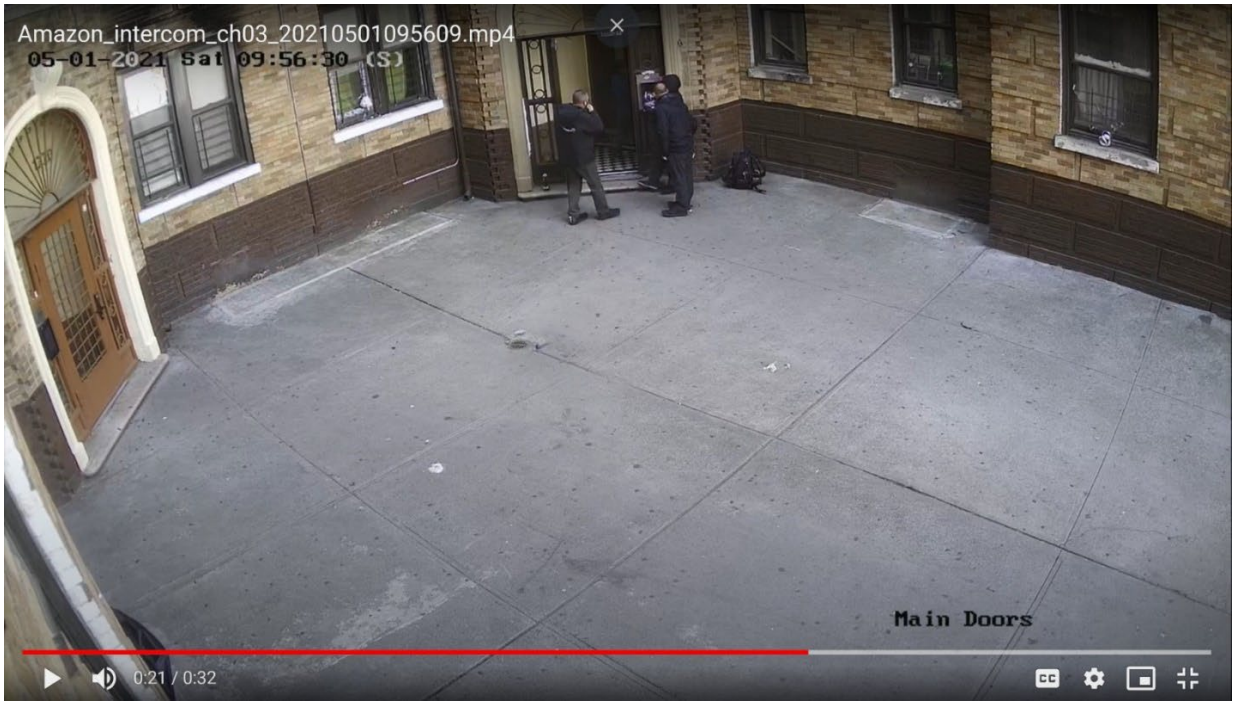
Displaying records 1 through 1 of 1.

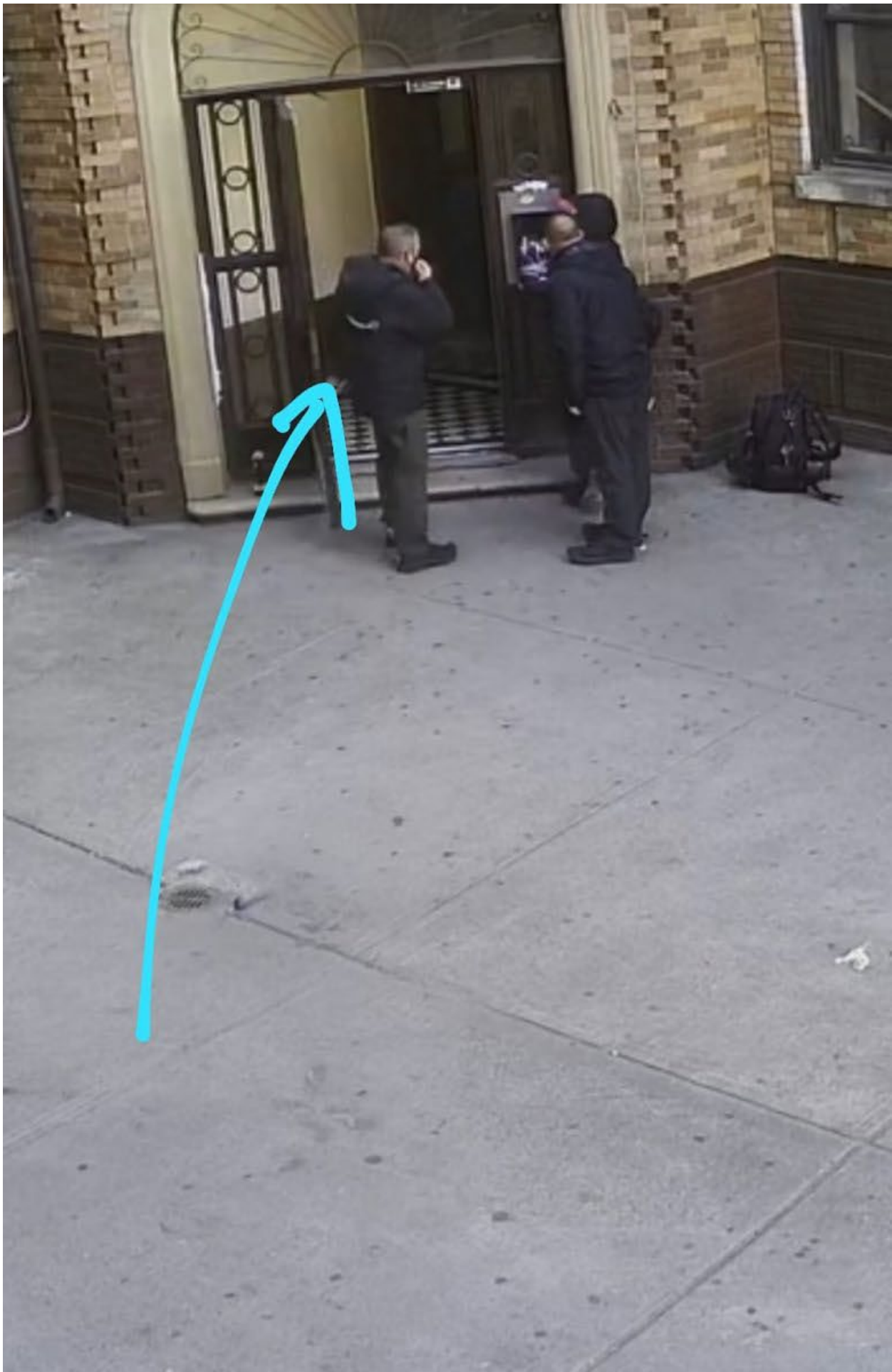
View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
	Detail Summary			Amazon .com Services, Inc.	410 Terry Ave. North	Seattle	WA	United States	98109	2AVOCKFBLORA	Change in Identification	03/03/2020	902.3	927.5

Perform Search Again

116. In addition, GateGuard has captured video of Amazon technicians tampering with multiple GateGuard devices.[22] Set forth below are images from the video showing Amazon technicians after they illegally opened the GateGuard® device without authorization and destroyed it:

[22] https://drive.google.com/file/d/1sFlE7808kHtjKajLsomDTwzTI3w1zlic/view
https://drive.google.com/file/d/1Xtry9xVKCv1-VRr2NyqpNvvDV03XjT4L/view

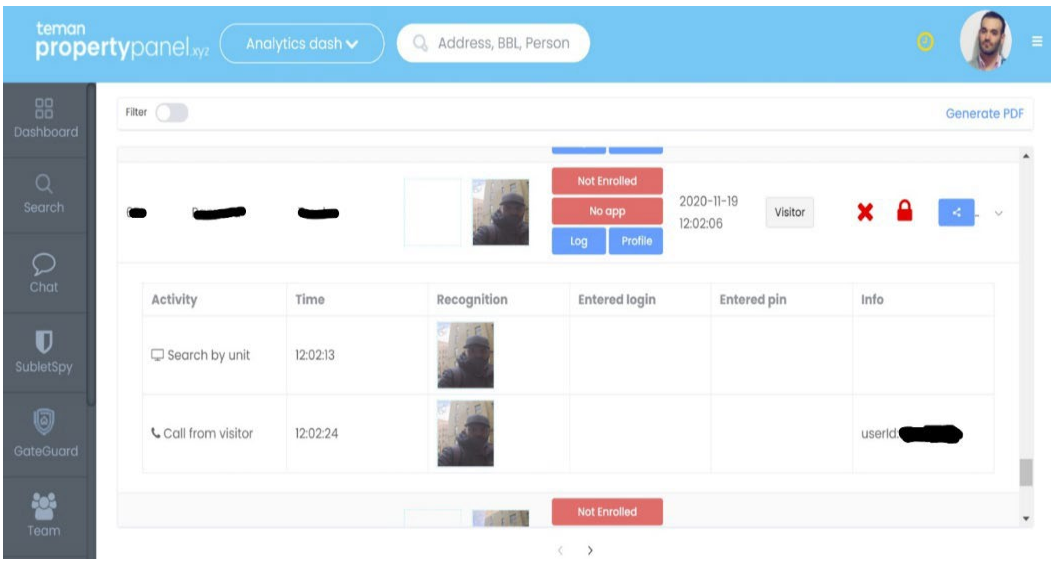

Amazon_intercom_ch03_20210501095609.mp4
05-01-2021 Sat 09:56:30 (S)
Main Doors
0:21 / 0:32

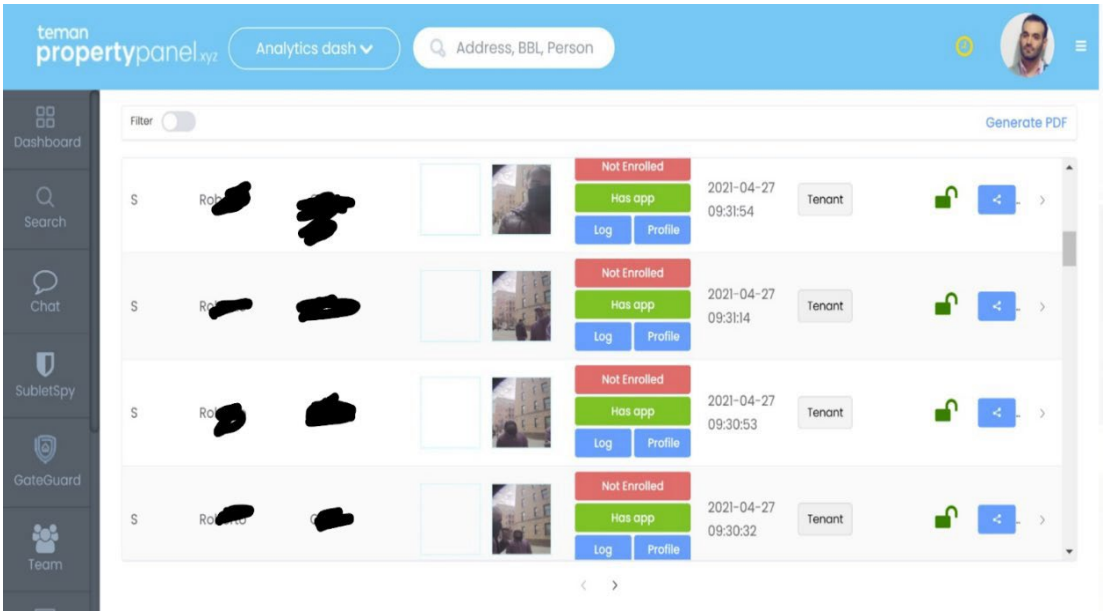


117. In the videos, Amazon employees wearing the jacket with the familiar Amazon prime half-moon ascending arrow logo can be seen installing a device into the existing intercom at a building served exclusively by GateGuard. Amazon did not obtain the consent of either GateGuard or the property owner for the installation of its Key.

Amazon's Key for Business Installations Routinely Damage Intercoms, Door Locks, and Wiring

118. On approximately 20 different occasions, building management have called GateGuard to repair or replace disabled intercom devices. These calls cost GateGuard time and money in support and repair, and it is likely that there are many more incidents that are not reported, causing even greater disruption to customers and loss of business.



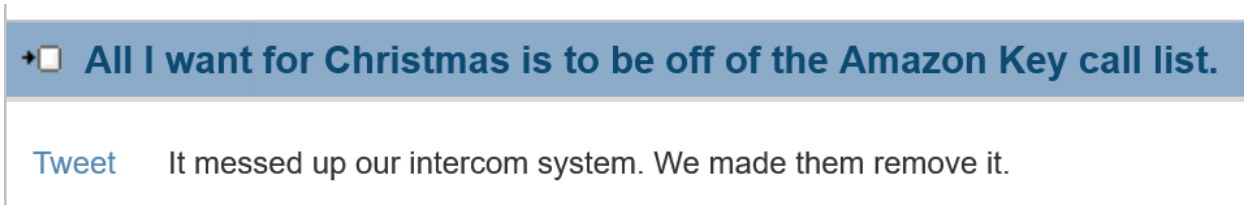


120. Each time GateGuard has been called by building management, GateGuard has discovered that Amazon tampered with its intercoms, including by inserting and connecting Amazon's extenders, a crucial component of the Key for Business "upgrade responsible for the damage described above.

121. On information and belief, Amazon's actions are not isolated instances, but are systematic business practices designed to destroy competition. The numerous on-line complaints and the confirmation that Amazon representatives lie about their authority to install equipment as discussed above provide a reasonable inference that Amazon's practices are widespread.

122. Amazon's strategy is then to disparage its competitors' device – that it has itself damaged, but without the property owners' consent – and propose the Amazon Key as an "upgrade" to a system "degraded" by the Key itself.

123. As shown in the Twitter dialogue reproduced below, when installing Key for Business – with or without authorization from building management – Amazon routinely disables or destroys existing intercom devices, door locks, and wiring:



124. After Amazon began aggressively seeking to control the building access market, GateGuard has received dozens of complaints and has been able to prove that these are directly related to Amazon's conduct.

125. As discussed below, GateGuard has confronted Amazon with evidence of its misconduct and, rather than compensating GateGuard for the damage caused, on information and belief, Amazon has profited from the information provided by GateGuard to surreptitiously reinstall its devices to cover up its initial illegal tampering. On information and belief, all of the customer complaints relating to GateGuard devices failing after an Amazon Key installation are a direct result of Amazon's conduct. In addition, many instances of illegal installation remain undiscovered, continuing to put GateGuard's equipment at risk (because some devices short repeatedly and only fail over time) and continuing to provide Amazon with unearned benefits from its illegal free-riding conduct.

126. As a result of Amazon's conduct, a number of GateGuard customers, residents and others have come to believe falsely that GateGuard's intercom systems are defective or that they are otherwise less desirable or valuable to building owners than the Amazon systems that have been illegally inserted into GateGuard intercoms. When the Key does not damage or destroy the device, Amazon also profits from its illicit activities.

Amazon Attempts to Avoid Detection

127. To prevent detection, particularly after it learns that a savvy access control provider such as GateGuard has become aware of its tactics, Amazon removes its "extenders" from GateGuard's devices after they have been sufficiently damaged.

128. GateGuard has been told by building managers that Amazon misleads them, claims the extenders had nothing to do with any malfunctioning of GateGuard's devices and then returns to the building to install a new device that it now presents as an "update" that will avoid the problems with the previous access control system. Since the property managers were in many, if not most situations, unaware of the initial installation, they can easily be duped by Amazon. Even

in rare situations where the property managers authorized the installation, they were not informed of the manner in which Amazon would install its Key directly into GateGuard's intercom or onto its wiring, leading the property managers to believe Amazon's lies that their product had nothing to do with GateGuard's malfunctioning. Landlord's properties' have also been damaged, as building amplifiers are blown out and the building magnetic door strikes are disabled by the surreptitious installation of the Key without property owners' and managers'

knowledge and consent.

129. As a result of Amazon's conduct, GateGuard has suffered reputational harm, diminished customer loyalty, and loss of revenue and other valuable commercial relationships, both existing and prospective.

Amazon Reveals its Intentions

130. In October of 2020, GateGuard approached Amazon and provided considerable evidence of its destructive and unlawful conduct (including the evidence incorporated above).

131. In addition to denying any responsibility for its conduct, Amazon "gaslit" GateGuard, suggesting that the failure of GateGuard devices identified as having been the result of tampering by Amazon was not because of anything done by Amazon but, rather, was GateGuard's fault.

132. Amazon's arguments to this effect, however, were unsubstantiated, unsupportable and false.

133. Although Amazon evinced interest in further discussions to explore a potential resolution, when the parties met, Amazon refused to cease installing Key for Business in a manner that damaged GateGuard and merely offered to enlist GateGuard as a Key for Business installer, for which GateGuard would be paid a nominal fee.

134. Amazon characterized the Hobson's choice it presented to GateGuard (which was recorded on video by GateGuard) along the lines of, "***either [Amazon] can cost you money or make you money***." This is exactly the strategy Amazon aims to deploy with other potential rivals,

turning itself into the essential gatekeeper, relegating third parties, at best, to an "adjunct" role and making it prohibitively expensive for others to provide rival and truly competitive access solutions. In the long run, this strategy aims not only to control the access market, but, ultimately, to control the ecommerce and package delivery markets generally.

Amazon Takes Its Theft of GateGuard's Trade Secrets Into Overdrive by Stealing the Intellectual Property Behind the Entire GateGuard System.

135. Not content to break into GateGuard's devices to observe their inner workings and modify the Key so that it would be "compatible" with GateGuard – without GateGuard's consent and in violation of GateGuard's Terms and Conditions – on or about March 8, 2023, Amazon instructed one of its channel partners to pose as a GateGuard client and obtain two devices for inspection by Amazon.

136. Amazon further instructed its channel partner to ship one device to the A2Z Development Center in Sunnyvale, CA and to ship one device to Ring in Las Vegas.

137. Once the device had been acquired, GateGuard naturally activated the device.

138. Thus by posing as a client, the channel partner was able to provide Amazon with an activated device that its engineers could use to hack into the GateGuard "back end" and thus observe the functioning of the GateGuard system as a whole, an not merely the functioning of the GateGuard intercom itself. that enables property management at residences under contract to GateGuard.

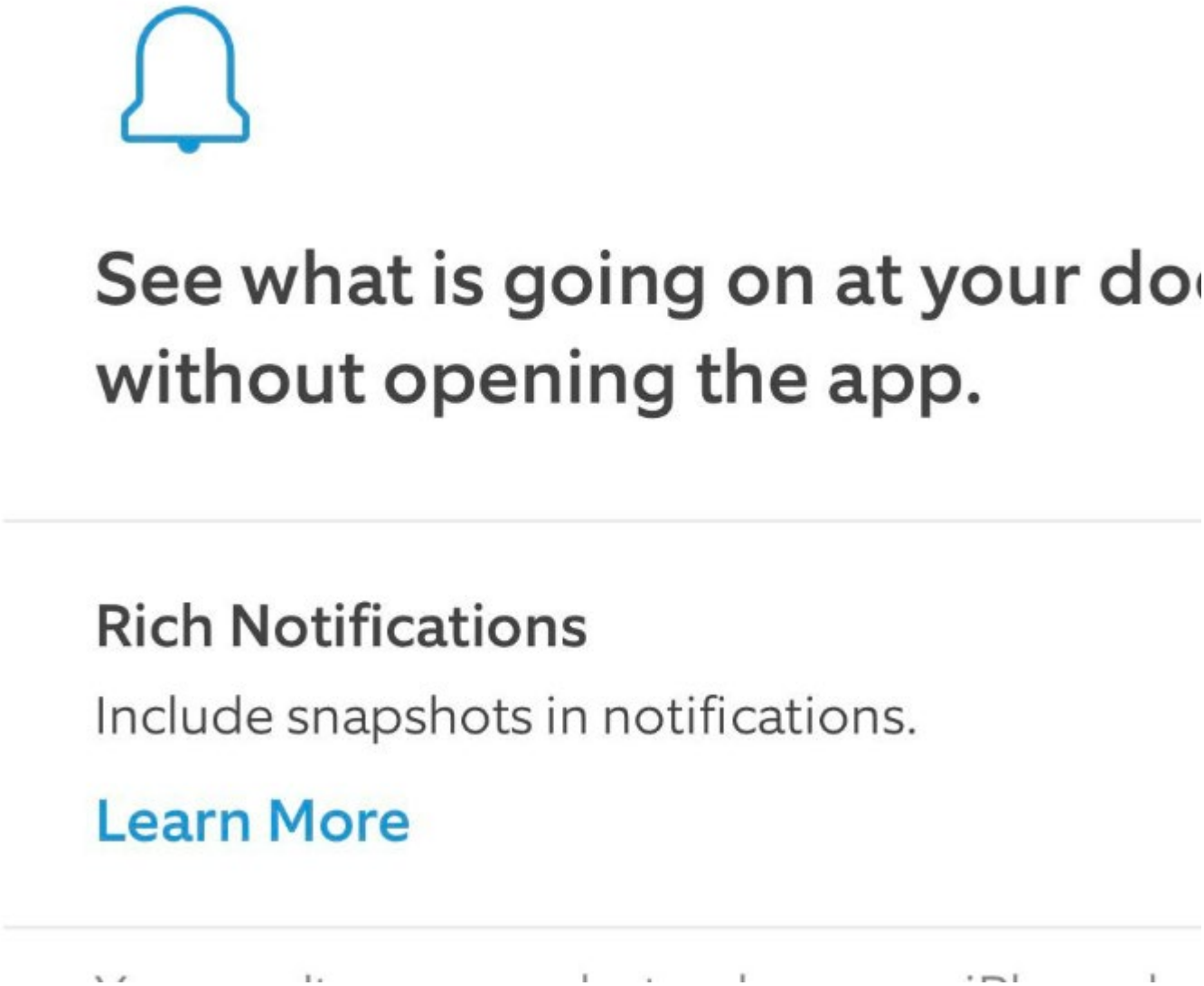
139. After examining, analyzing, and testing the GateGuard device, the Key for Business rolled out a new service, transforming the Key device from a door unlocking service for Amazon deliverers to a property management tool for property managers. Amazon is thus using its

knowledge of the GateGuard system specifically to target the customers of GateGuard and others serving the property management market.

140. The new service is specifically defined by Amazon as a "web-based portal for property managers to manage third party provider access," as described in more detail in paragraph 12 above. This service closely parallels GateGuard's Property Panel, available as part of the GateGuard system that Amazon had access to at its research and development center after the device was shipped to the center in March 2021.

141. Most importantly, at the time that Amazon illegally acquired one of GateGuard's activated devices and sent it to its secret Ring-controlled research laboratory, Ring was in the process of testing compatibility of third-party intercoms with its new Ring Intercom that it began marketing in 2021. Ring was able to observe the functioning of the GateGuard devices and modify the Ring Intercom to incorporate elements of the GateGuard system and also refine the integration of its Ring Intercom that was designed for the European market where a device such as the Ring Intercom would need to integrate with a wide variety of existing intercom systems. Naturally, Amazon did not inform GateGuard of its use of its device.

142. Instead, once Amazon had used the device for its own purposes, it destroyed the GateGuard device to definitively bury its tracks.

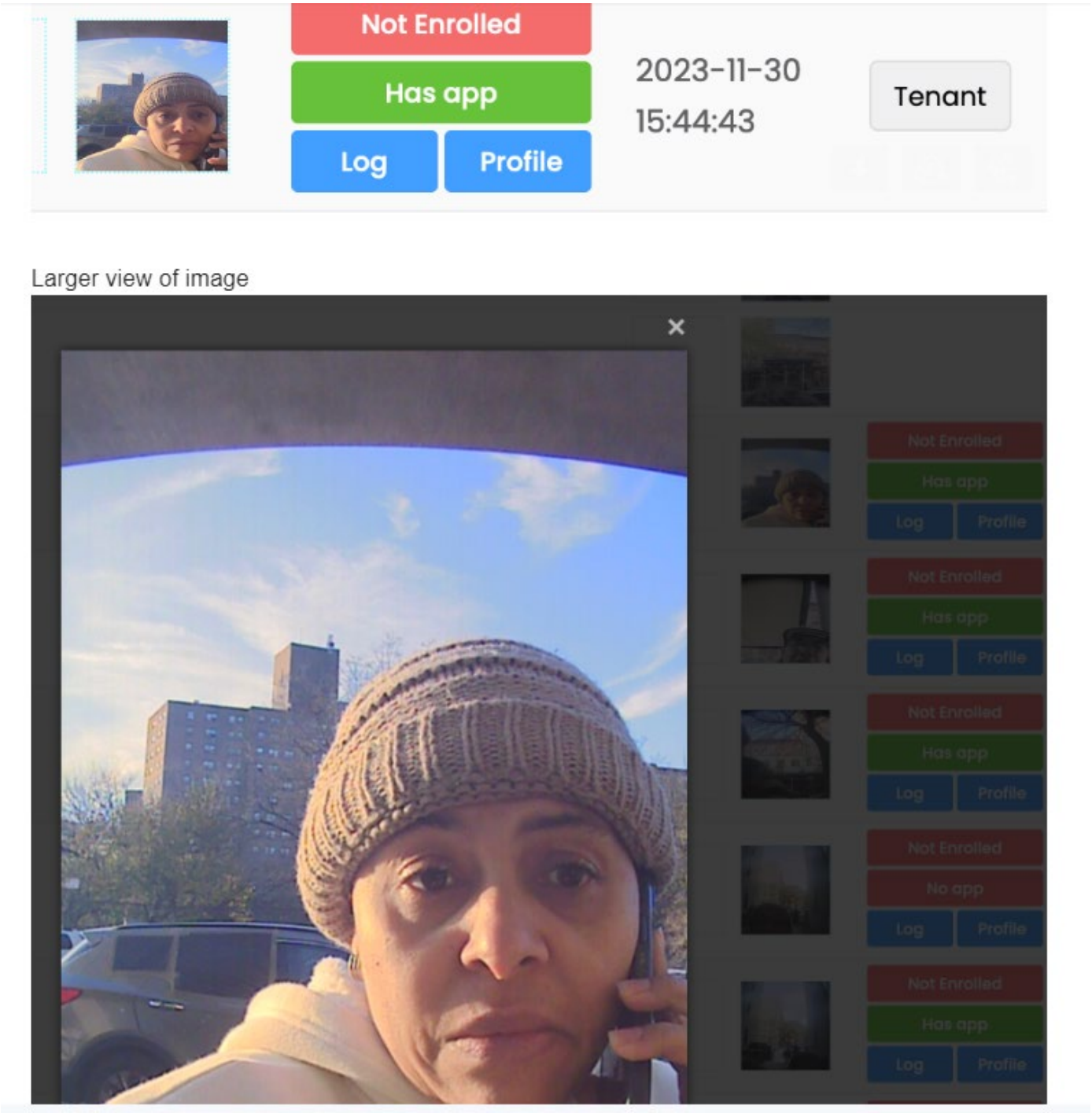


143. Set forth below are images showing the functioning of the later-introduced Ring "rich notification":

144. "When you receive a Rich Notification you will see a small image, this is the snapshot of the event. You can enlarge this directly from the push notification. As Amazon describes the feature:

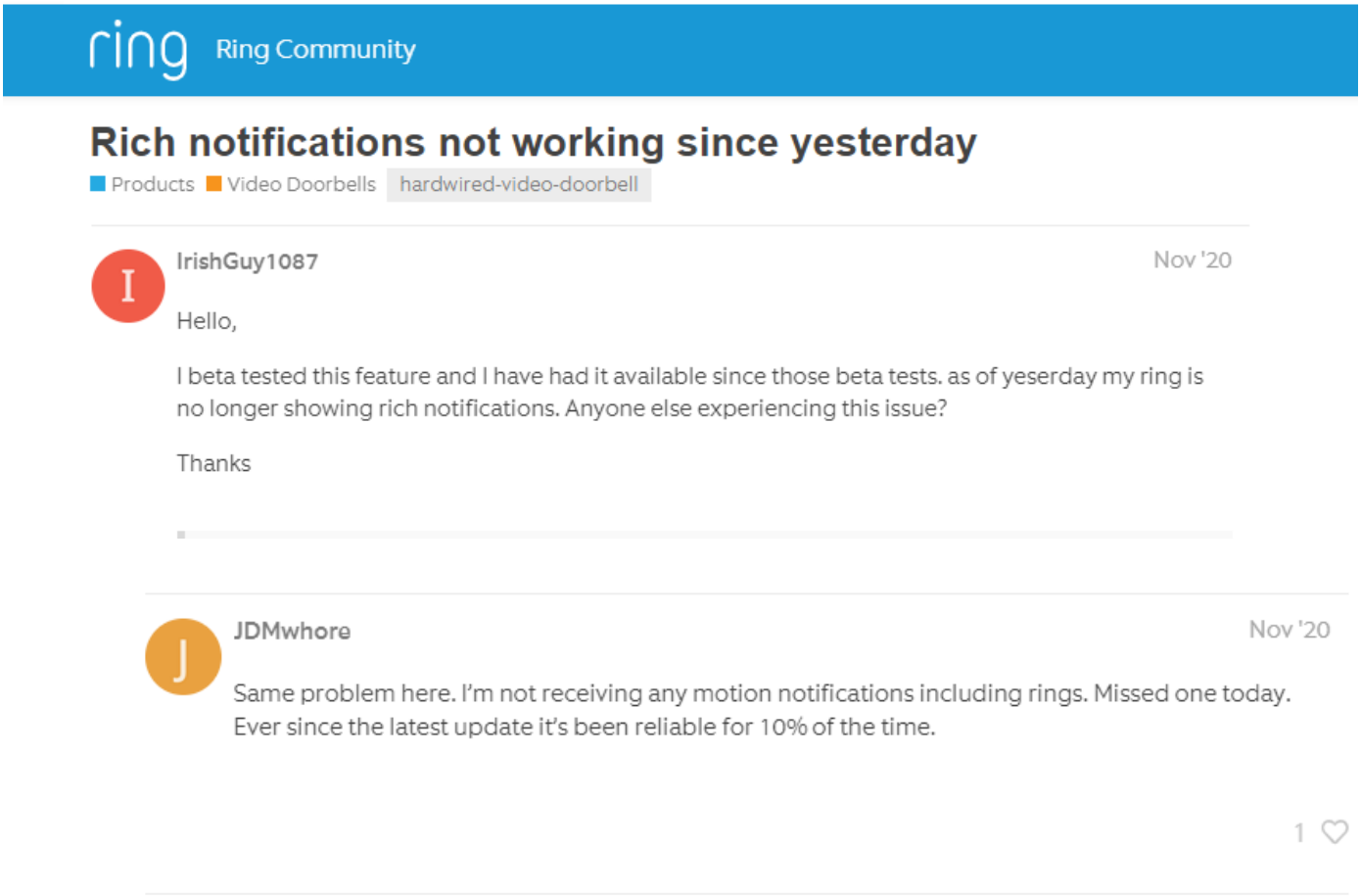
145. Like Ring, GateGuard offers a "rich notification" feature to its users, developed before the Ring was introduced and with higher reliability and greater resolution.

146. Set forth below is an image of the GateGuard feature, showing the device video capture being sent as a still image to a user's mobile phone:



147. However, Ring encountered numerous problems and "bugs" in its roll-out of the Ring, leading to

extensive consumer complaints. https://community.ring.com/t/rich-notifications-not-working-since-yesterday/18722.



ring Ring Community

Rich notifications not working since yesterday

Products Video Doorbells hardwired-video-doorbell

I IrishGuy1087 Nov '20

Hello,

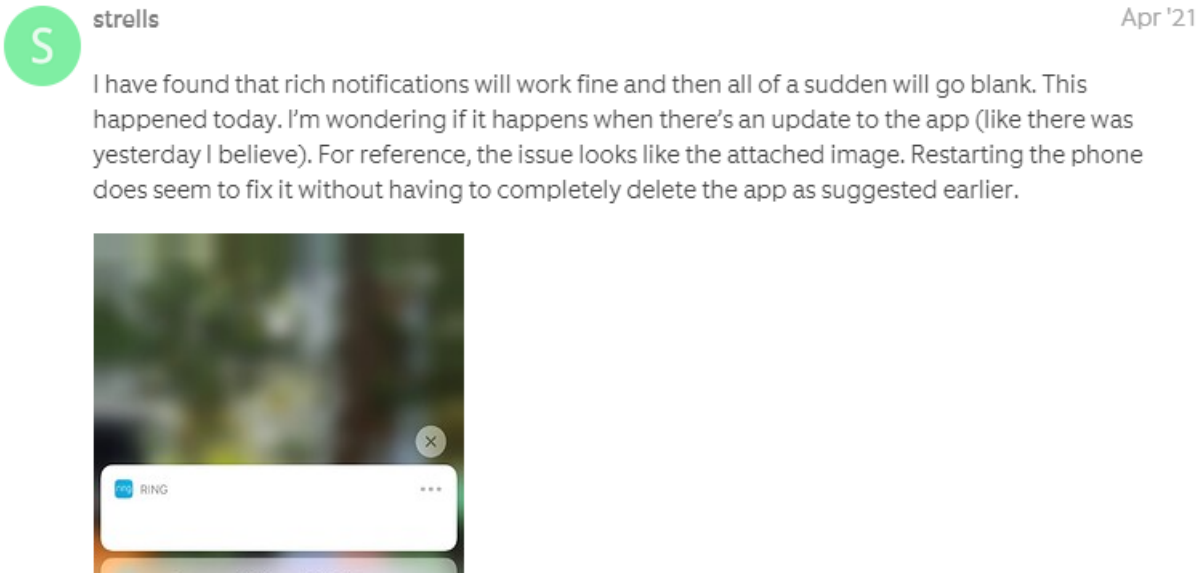
I beta tested this feature and I have had it available since those beta tests. as of yeserday my ring is no longer showing rich notifications. Anyone else experiencing this issue?

Thanks

J JDMwhore Nov '20

Same problem here. I'm not receiving any motion notifications including rings. Missed one today. Ever since the latest update it's been reliable for 10% of the time.

1 ♡



Summary of Amazon's Anti-Competitive Conduct

148. Amazon is not achieving dominance of the building access and e-commerce delivery markets by technological innovation, but by deception, harassment, ruthlessness, and blatantly illegal conduct, such as the unauthorized accessing of and tampering with GateGuard and other parties' devices, and the pattern of lies and misrepresentations through which it deceives lower-level apartment personnel to permit installation of the Key without the need to contact and consult the "higher-ups."

149. The House Antitrust Report documents Amazon's brazenly anti-competitive behavior, highlighting Amazon's bullying, appropriation of third-party seller data, imposing fees on captive users of its platforms, "self-preferencing" and abusing its "gatekeeper power." Much of the House Antitrust Report evokes patterns strikingly similar to the conduct that has so damaged GateGuard, and underscores the anti-competitive purpose underlying Amazon's deceptive, illegal and cut-throat practices: "Once Amazon succeeds in trapping enough customers in its "flywheel" to secure dominant position across varied markets, it can then raise prices or remove incentives or allowances for third party sellers/competitors." Damning as it is, however, the

House Antitrust Report is not the only source of information for Amazon's history of anti-competitive practices.

150. Reuters recently reported that it had reviewed thousands of pages of internal Amazon documents – including emails, strategy papers and business plans – that show the company ran a systematic campaign of creating knockoffs and manipulating search results to boost its own product lines in India, one of the company's largest growth markets. The documents reveal how Amazon's private-brands team in India secretly exploited internal data from Amazon.in to copy products sold by other companies, and then offered them on its platform.[23] On information and belief, Amazon has stolen GateGuard's proprietary data in a similar manner.

151. The conduct of which GateGuard and others have been victim in fact represents the anti-competitive DNA at the core of the Amazon business model.

CAUSES OF ACTION

COUNT I.

COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1030 *et seq*.) (AS TO ALL DEFENDANTS)

152. GateGuard realleges and incorporates by reference each and every allegation set above.

153. GateGuard's devices are "high speed data processing device performing logical, arithmetic, or storage functions" and thus come within the definition of "computer" under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e)(1).

154. GateGuard's intercom devices are involved in interstate and foreign commerce because they control packages and other deliveries to residential dwellings that originate from locations both inside and outside of the State of New York. As a result, GateGuard's intercoms are "protected

computers" under 18 U.S.C. § 1030(e)(2).

[23] https://www.reuters.com/investigates/special-report/amazon-india-rigging/

155. Upon information and belief, Defendants knowingly and intentionally accessed GateGuard's intercom devices without authorization or in excess of authorization, and thereby obtained and used valuable information from those devices, including customer locations, accounts, and id's, in violation of 18 U.S.C. § 1030(a)(2)(C).

156. Upon information and belief, Defendants intentionally accessed a protected computer or computers without authorization, and as a result of such conduct, caused damage and loss, in violation of 18 U.S.C. § 1030(a)(5)(C), or recklessly caused damage in violation of 18 U.S.C. § 1030(a)(5)(B).

157. Defendants caused loss to one or more persons during a one-year period aggregating well over $5,000 in value, and they also caused damage affecting ten or more protected computers during a one-year period under 18 U.S.C. § 1030(c)(4)(A)(i)(I).

158. Amazon's imposition of ever-increasing delivery quotas as part of its illegal scheme described herein poses a direct threat to public health and safety, harming both the drivers and installers and also leading to reckless driving conduct, in violation of 18 U.S.C. § 1030(c)(4)(A)(i)(4).

159. GateGuard has suffered damage and loss as a consequence of Defendants' actions, including but not limited to the cost of investigating and responding to unauthorized access and abuse of its intercom devices, conducting damage assessments, restoring and replacing intercom devices, wiring, systems, or information, termination of contracts, the loss of existing and future business, the interference with GateGuard's uploading and preservation of proprietary data, and the harm to GateGuard's operations, reputation and goodwill as described above, all in an amount to be determined at trial, but no less than FORTY MILLION DOLLARS ($40,000,000) together with attorneys' fees and other equitable relief under 18 U.S.C. § 1030(g).

COUNT II.

TORTIOUS INTERFERENCE WITH CONTRACT UNDER NEW YORK LAW (AS TO ALL DEFENDANTS)

160. GateGuard realleges and incorporates by reference each and every allegation set forth in the foregoing paragraphs above.

161. GateGuard has entered into valid contracts with the owners or authorized agents of the residential dwellings at which Plaintiff's intercom devices were installed.

162. Defendants were aware of these contracts as evidenced by their misrepresentation of their authority to access and tamper with Gateguard's devices.

163. Defendants intentionally procured the breach of GateGuard's contracts with landlords and property managers by causing the intercom devices to malfunction and the causing the termination of contracts with GateGuard under false pretexts. In fact, GateGuard's contracts do not permit termination when the devices have been damaged by a third party due to no fault of GateGuard's.

164. Plaintiff has suffered damages as a result of Defendant's intentional interference with their contractual relations with landlords and their agents in an amount to be determined at trial, but no less than TWENTY-SEVEN MILLION DOLLARS ($27,000,000).

COUNT III.

TORTIOUS INTERFERENCE WITH PROSPECTIVE ECONOMIC ADVANTAGE UNDER NEW YORK LAW (AS TO ALL DEFENDANTS)

165. GateGuard realleges and incorporates by reference each and every allegation set forth in the foregoing paragraphs above.

166. Defendants intentionally and wrongfully interfered with future economic advantage to be received from existing customers through the extension of their contracts with Plaintiff and from future customers who will be deceived into thinking Plaintiff's rival product to the Key for Business is responsible for the equipment malfunctioning.

167. Plaintiff has lost existing customers, future business from such customers and prospective customers as a result of Defendants' wrongful conduct, including their unauthorized access to Plaintiff's intercom devices and their tampering with and manipulating said devices to cause them to malfunction.

168. Plaintiff has also been delayed in fulfilling new, revenue-generating devices as its installers were forced to rush to repair extensive damage caused by Amazon's illegal installations, losing that revenue-generating time forever.

169. As a result of Defendants' tortious interference with prospective economic advantage, Plaintiff has suffered damages in an amount to be determined at trial, but no less than FOURTY MILLION DOLLARS ($40,000,000).

COUNT IV.

TRESPASS TO CHATTELS UNDER NEW YORK LAW
(AS TO ALL DEFENDANTS)

170. GateGuard realleges and incorporates by reference each and every allegation set forth in the foregoing paragraphs above.

171. Defendants intentionally impaired the condition, quality and value of Plaintiff's intercom devices by means of their unauthorized access to such devices and their manipulation and tampering with the devices in such a manner as to impair their proper functioning and deprive Plaintiff of the economic benefit therefrom.

172. As a result of Defendants' intentional impairment of the condition, quality and value of Plaintiff's intercom devices, Defendants have committed trespass to chattels and are liable to Plaintiff for damages in an amount to be determined at trial, but no less than TEN MILLION DOLLARS ($10,000,000).

COUNT V.

CONVERSION
(AS TO ALL DEFENDANTS)

173. GateGuard realleges and incorporates by reference each and every allegation set forth in the foregoing paragraphs above.

174. GateGuard is the legal owner of the intercom devices installed at residential dwellings under contract with it.

175. By accessing GateGuard's intercoms without authorization and using and misusing the devices so as to install the Key for Business, Defendants wrongfully exercised dominion over Plaintiff's intercom devices.

176. As a result of the ensuing conversion of Plaintiff's property, Plaintiff has suffered damages in an amount to be determined at trial, but no less than TEN MILLION DOLLARS ($10,000,000)

COUNT VI.

MISAPPROPRIATION OF TRADE SECRETS UNDER NEW YORK LAW
(AS TO ALL DEFENDANTS)

177. GateGuard realleges and incorporates by reference each and every allegation set forth in the foregoing paragraphs above.

178. GateGuard possesses trade secrets in its intercom devices, including the configuration of its motherboard, the placement and type of electronic circuitry and other

components used, the insulation resistance between circuits, the voltages at which the device operates, the mechanisms of internet connectivity, the antennae used, the inner casing of the intercom, its system of wall-mounting and hinges, its waterproofing design, and its custom-designed cables.

179. This proprietary technology is kept secret from competitors and customers, with only authorized GateGuard agents permitted access to the devices for repairs and troubleshooting. GateGuard developed its devices after thousands of hours of trial and error and years of painstaking research and development, including by its founder Ari Teman, who sacrificed his personal life and health to develop GateGuard's technology. The Company's trade secrets are the core of its value, which has been established at $300 million for purposes of the Company's most recent round of fundraising. Without acquiring GateGuard or illegally accessing the GateGuard devices, Amazon would be unable to develop a device with the same or similar functionality.

180. Defendants wrongfully and dishonestly, by means of subterfuge, deceit, and other illegal conduct, misappropriated Plaintiff's trade secrets, applied Plaintiff's intercom devices to their own use, accessing the inner workings of the GateGuard devices and installing Key extenders without authorization, paying compensation or obtaining consent

181. As a result of Defendants' wrongful misappropriation of Plaintiff's trade secrets, Plaintiff has suffered damages in an amount to be determined at trial, but no less than ONE HUNDRED MILLION DOLLARS ($100,000,000).

COUNT VII

VIOLATION OF THE DEFEND TRADE SECRETS ACT OF 2016, 18 U.S.C.A. § 1832 et seq., (AS TO ALL DEFENDANTS)

182. GateGuard realleges and incorporates by reference each and every allegation set forth in the foregoing paragraphs above.

183. By illegally wiring into GateGuard's intercoms, Amazon has been able to misappropriate valuable proprietary intellectual property, as described in paragraphs 86 and 165 above.

184. GateGuard maintains and protects the secrecy of the foregoing information and only provides access to authorized users pursuant to express contract or agreement.

185. GateGuard is the owner of the intellectual property in its devices, including the associated trade secrets.

186. GateGuard devoted thousands of hours and years of research and development to develop the GateGuard intercom.

187. Defendants did, with intent to convert a trade secret, related to a product or service used in or intended for use in interstate or foreign commerce, to its own unauthorized economic benefit, and knowing that said conversion would injure GateGuard,

- steal, or without authorization appropriate, take, carry away, or conceal, or by fraud, artifice, or deception obtain GateGuard trade secrets;
- without authorization copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, or convey GateGuard trade secrets; and/or
- attempt to commit the foregoing.

188. As a result of Defendants' willful and malicious conduct, GateGuard has suffered damages, including exemplary damages equal to two times its actual damages, in an amount to be determined at trial, but no less than TWO HUNDRED MILLION DOLLARS ($200,000,000) together with the payment of attorney's fees and costs.

COUNT XI – CLASS CLAIM.

TRESPASS AND CONVERSION TORTIOUS INTERFERENCE WITH PROSPECTIVE ECONOMIC ADVANTAGE (AS TO ALL DEFENDANTS)

189. GateGuard realleges and incorporates by reference each and every allegation set forth in the foregoing paragraphs above.

190. Every property owner or property package management service has a legal and economic interest in controlling access to its buildings. Access to its buildings for package delivery services is, for Amazon, a billion dollar plus business that provides enormous cost savings and a tremendous competitive advantage. Amazon, however, does not own access control rights: these are owned by the individual buildings to which access is sought or to other entities, such as GateGuard, with which the property has contracted for package delivery management services. In a competitive market functioning without lies and subterfuge, **i**f it wanted preferential access to residential buildings, Amazon would be required to purchase access to buildings from those with the legal and economic rights control access. The price charged for such access would be set as a function of the value of the access to Amazon. By illegally and through subterfuge bypassing the landlords, property managers and package management services, there is an enormous wealth transfer to Amazon that is unearned by any innovation but is rather made possible by the pattern of installing the Amazon Key without authorization from those parties with true legal rights to control and charge for access to the buildings to which Amazon surreptitiously gains access.

191. Amazon thus robs those with the legal right to charge for access to property of a clear economic expectancy, as it is evident that access rights have a definite value that the owner can

expect to bargain for.

192. Defendants intentionally and wrongfully interfered with future economic advantage to charge Amazon for building access the price that would be set for such access in a competitive market operating without lies and subterfuge and have damaged the property of landlords and third parties**.**

193. Plaintiffs have lost a clear and concrete revenue stream by Amazon's diversion to itself of the economic value of building access and its capturing of the value of such access without the legal owners' or right holders' consents.

194. There are hundreds if not thousands of property owners, property managers and other access control rights holders who have been harmed by Amazon's surreptitious capturing of the economic value of building access and damage to their property to the detriment of such owners, managers and other rights holders.

195. As a result of Defendants' tortious interference with their prospective economic advantage, trespass and conversion GateGuard and the other members of the class are entitled to treble damages in an amount to be determined at trial but no less than ONE BILLION DOLLARS ($1,000,000,000), together with attorneys' fees and costs.

CLASS REPRESENTATION ALLEGATIONS

196. The Class Members are so numerous that their individual joinder herein is impracticable. On information and belief, the Class Members number in the thousands. Members of the class include property owners, property managers and package delivery and management services who have suffered similar injury toGateGuard. The precise number of Class Members and their identities are unknown at this time but may be determined through discovery. Class Members may be notified of the pendency of this action by mail and/or publication through the records of Defendants.

197. Common questions of law and fact exist as to all Class Members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to, the extent to which Amazon and its representatives obtained access to buildings without the authorization of the true owners of access rights, whether by outright fraud, connivance or gross recklessness.

120. The claims of GateGuard are typical of the claims of the Class Members in that GateGuard had contracted with property managers for the right to control, monitor and regulate building access for the benefit of the property managers, and was bypassed by Amazon's system of deceit and subterfuge that enable the installation the Amazon Key and the resulting control of building access without GateGuard's control, in the same that property managers and property owners are deprived of their right to control, monitor, regulate and profits from third-party access to their buildings. All class members must prove Amazon's pattern of deceit illegally accessing properties without the consent of the access control rights holder such as GateGuard.

198. GateGuard is an adequate representative of the Class because its interests do not conflict with the interests of the Class Members it seeks to represent, it has retained competent counsel experienced in prosecuting class actions, and it intends to prosecute this action vigorously.

199. The interests of Class Members will be fairly and adequately protected by Plaintiff and its counsel.

200. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendants' liability, particularly against an entity such as Amazon that has a virtually unlimited budget for its legal defense. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendants' liability.

JURY DEMAND

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff demands a trial by jury.

WHEREFORE, Plaintiff demands judgment:

(1) Under Count I, for damages resulting from Defendants' violation of the Computer Fraud and Abuse Act in an amount to be determined at trial, but no less than FORTY MILLION DOLLARS ($40,000,000), together with attorneys' fees and costs.

(2) Under Count II, for damages resulting from Defendants' tortious interference with contract in an amount to be determined at trial, but no less than TWENTY-SEVEN MILLION DOLLARS ($27,000,000), together with attorneys' fees and costs.

(3) Under Count III, for damages resulting from Defendants' tortious interference with prospective economic advantage in an amount to be determined at trial, but no less than FORTY MILLION DOLLARS ($40,000,000), together with attorneys' fees and costs.

(4) Under Count IV, for damages resulting from Defendants' trespass to chattels in an amount to be determined at trial, but no less than TEN MILLION DOLLARS ($10,000,000).

(5) Under Count V, for damages resulting from Defendants' conversion of Plaintiff's property in an amount to be determined at trial, but no less than TEN MILLION DOLLARS ($10,000,000), together with attorneys' fees and costs.

(6) Under Count VI, for damages resulting from Defendants' wrongful misappropriation of Plaintiff's trade secrets in an amount to be determined at trial, but no less than ONE HUNDRED MILLION DOLLARS ($100,000,000).

(7) Under Count VII, for damages, including double damages for Amazon's willful and malicious conduct, for violation of the Defend Trade Secrets Act in an amount to be determined at trial, but no less than TWO HUNDRED MILLION DOLLARS ($200,000,000), together with attorneys' fees and costs.

(8) Certifying Count VIII as a class action under Rule 23(b)(3) of the Federal Rules of Civil Procedure Rule and appointing GateGuard as class representative.

(9) Awarding GateGuard a reasonable fee as class representative.

(10) Issuing an injunction permanently enjoining Defendants from accessing Plaintiff's intercom devices without authorization, modifying, altering or tampering with such devices in any manner without Plaintiff's express authorization, and accessing any properties without the consent of the property owner, manager or other authorized rights holder

(11) Such other relief as this Court deems just and proper.

Dated: New York, New York
August 1, 2024

QUAINTON LAW, PLLC
2 Park Ave., 2nd Floor
New York, New York 10016
(212) 419-0575
Attorneys for Plaintiff
GateGuard, Inc.

By: */s/ Eden P. Quainton*
EDEN P. QUAINTON